OCTAVE®-S Implementation Guide, Version 1.0

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

HANDBOOK
CMU/SEI-2003-HB-003

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

OCTAVE®-S Implementation Guide, Version 1.0

Volume 1: Introduction to OCTAVE-S

CMU/SEI-2003-HB-003

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

Networked Systems Survivability Program

This report was prepared for the

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

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

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

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

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

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

Table of Contents

List of Figures

List of Tables

About This Document

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

The volumes in this handbook are

- ***Volume 1: Introduction to OCTAVE-S*** – This volume provides a basic description of OCTAVE-S and advice on how to use the guide.
- *Volume 2: Preparation Guidelines* – This volume contains background and guidance for preparing to conduct an OCTAVE-S evaluation.
- *Volume 3: Method Guidelines* – This volume includes detailed guidance for each OCTAVE-S activity.
- *Volume 4: Organizational Information Workbook* – This volume provides worksheets for all organizational-level information gathered and analyzed during OCTAVE-S.
- *Volume 5: Critical Asset Workbook for Information* – This volume provides worksheets to document data related to critical assets that are categorized as information.
- *Volume 6: Critical Asset Workbook for Systems* – This volume provides worksheets to document data related to critical assets that are categorized as systems.
- *Volume 7: Critical Asset Workbook for Applications* – This volume provides worksheets to document data related to critical assets that are categorized as applications.
- *Volume 8: Critical Asset Workbook for People* – This volume provides worksheets to document data related to critical assets that are categorized as people.
- *Volume 9: Strategy and Plan Workbook* – This volume provides worksheets to record the current and desired protection strategy and the risk mitigation plans.
- *Volume 10: Example Scenario* – This volume includes a detailed scenario illustrating a completed set of worksheets.

Acknowledgements

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

Abstract

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

1 Purpose and Scope

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

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

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

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

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

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

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

2 What Is OCTAVE-S?

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

2.1 Overview of the OCTAVE Approach

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

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

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

2.2 Overview of OCTAVE-S

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

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

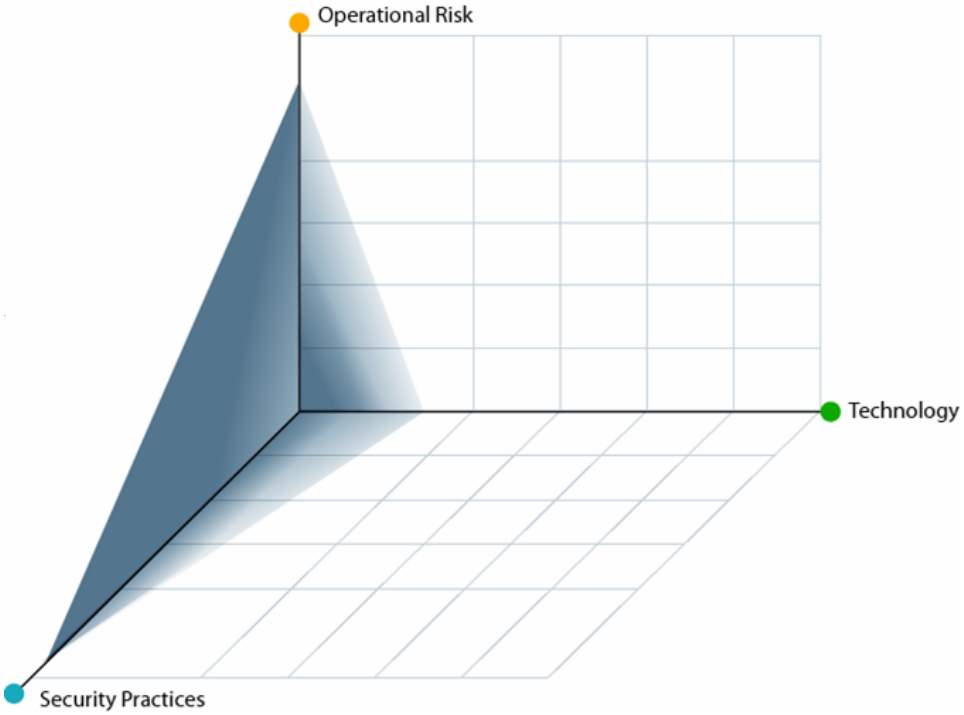


Figure 1: OCTAVE-S Emphasizes Operational Risk and Security Practices

Table 1: Key Differences Between OCTAVE and Other Approaches

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

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

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

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

2.3 OCTAVE-S Process

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

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

2.3.1 Phase 1: Build Asset-Based Threat Profiles

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

2.3.2 Phase 2: Identify Infrastructure Vulnerabilities

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

Table 2: Processes and Activities of Phase 1

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

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

Table 3: Processes and Activities of Phase 2

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

2.3.3 Phase 3: Develop Security Strategy and Plans

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

2.4 OCTAVE-S Outputs

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

Table 4: Processes and Activities of Phase 3

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

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

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

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

Other useful outputs of OCTAVE-S include

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

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

2.5 Scope of Application

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

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

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

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

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

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

2.5.1 Should You Use OCTAVE-S?

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

- Is your organization small? Does it have a flat or simple hierarchical structure?
- Can you find a group of three to five people for the analysis team who have a broad and deep understanding of the company and also possess most of the following skills?
  - problem-solving ability
  - analytical ability
  - ability to work in a team
  - at least one member with leadership skills
  - ability to spend a few days working on this method
- Do you outsource all or most of your information technology functions?
- Do you have a relatively simple information technology infrastructure that is well understood by at least one individual in your organization?
- Do you have limited familiarity with vulnerability evaluation tools within the context of information-related assets or are you unable to obtain the use of this expertise from current service provider to interpret results?

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

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

2.5.2 Words of Caution

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

3 Available Materials

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

- *Volume 1: Introduction to OCTAVE-S* – This volume provides a basic description of OCTAVE-S and advice on how to use the guide.
- *Volume 2: Preparation Guidelines* – This volume contains background and guidance for preparing to conduct an OCTAVE-S evaluation.
- *Volume 3: Method Guidelines* – This volume includes detailed guidance for each OCTAVE-S activity.
- *Volume 4: Organizational Information Workbook* – This volume provides worksheets for all organizational-level information gathered and analyzed during OCTAVE-S.
- *Volume 5: Critical Asset Workbook for Information* – This volume provides worksheets to document data related to critical assets that are categorized as information.
- *Volume 6: Critical Asset Workbook for Systems* – This volume provides worksheets to document data related to critical assets that are categorized as systems.
- *Volume 7: Critical Asset Workbook for Applications* – This volume provides worksheets to document data related to critical assets that are categorized as applications.
- *Volume 8: Critical Asset Workbook for People* – This volume provides worksheets to document data related to critical assets that are categorized as people.
- *Volume 9: Strategy and Plan Workbook* – This volume provides worksheets to record the current and desired protection strategy and the risk mitigation plans.
- *Volume 10: Example Scenario* – This volume includes a detailed scenario illustrating a completed set of worksheets.

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

3.1 Navigation Aid for Downloadable Materials

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

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

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

Process Chart

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

Process Chart (cont.)

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

Process Chart (cont.)

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

Process Chart (cont.)

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

Process Chart (cont.)

Process S3: Examine Computing Infrastructure in Relation to Critical Assets (cont.)

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

Process Chart (cont.)

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

Process Chart (cont.)

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

3.2 Additional Sources of Help

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

For other information, see also

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

References

[Alberts 01a] Alberts, Christopher and Dorofee, Audrey. *OCTAVE Method Implementation Guide, V2.0*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001. <http://www.cert.org/octave>.

[Alberts 01b] Alberts, Christopher and Dorofee, Audrey. *OCTAVE Criteria V2.0*. (CMU/SEI-2001-TR-016, ADA3399229). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001. <http://www.sei.cmu.edu/publications/documents/01.reports/01tr016.html>.

[Alberts 01c] Alberts, Christopher; Dorofee, Audrey; and Allen, Julia. *OCTAVE Catalog of Practices, V2.0*. (CMU/SEI-2001-TR-020, ADA 396654). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001. <http://www.sei.cmu.edu/publications/documents/01.reports/01tr020.html>.

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

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

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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

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

6. AUTHOR(S)

Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody

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

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

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

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

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

16. PRICE CODE

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

OCTAVE®-S Implementation Guide, Version 1.0

Volume 2: Preparation Guidance

Christoper Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

HANDBOOK
CMU/SEI-2003-HB-003

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

OCTAVE®-S Implementation Guide, Version 1.0

Volume 2: Preparation Guidance

CMU/SEI-2003-HB-003

Chrstopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

Networked Systems Survivability Program

This report was prepared for the

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

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

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

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

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

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

Table of Contents

List of 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℠ (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 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

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

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
OCTAVE-S Implementation Guide, Version 1.0, Volume 2	F19628-00-C-0003

6. AUTHOR(S)

Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody

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

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

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

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

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

16. PRICE CODE

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

OCTAVE®-S Implementation Guide, Version 1.0

Volume 3: Method Guidelines

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

HANDBOOK
CMU/SEI-2003-HB-003

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

OCTAVE®-S Implementation Guide, Version 1.0

Volume 3: Method Guidelines

CMU/SEI-2003-HB-003

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

Networked Systems Survivability Program

This report was prepared for the

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

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

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

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

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

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

Table of Contents

List of Tables

About This Document

This document is Volume 3 of the *OCTAVE-S Implementation Guide*, a 10-volume handbook supporting the OCTAVE-S methodology. This volume provides the detailed guidelines for conducting 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℠ (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.

Introduction

This document contains the Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE®)-S method guidance. This volume provides detailed guidelines and some specific examples for each activity in OCTAVE-S. A complete example showing the key worksheets and results is provided in Volume 10 and can be used as an aid in understanding the method guidance. The worksheets referred to in the guidance are all contained in Volumes 4 through 9 of this handbook.

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

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

Activities Applicable to All Phases and Processes

The following activities can occur during any phase or process of OCTAVE-S:

- Develop action list
- Document notes and recommendations

Develop Action List

Develop Action List	All Phases, All Processes, All Steps

Activity Worksheets	*Reference Worksheets*
• Action List (Vol. 9)	• none

Background/Definitions

Action list – a list of near-term action items identified during OCTAVE-S activities

An action item is something that an organization intends to complete in the near term. Action items generally don't require

- specialized training
- policy changes
- changes to roles and responsibilities

Instructions

During the evaluation, you will likely identify near-term actions that need to be completed. As you identify an action item, document that action on the *Action List Worksheet* (Vol. 9). Include the following information for each action item:

- a description of the action
- responsibility for completing the action
- a date for completing the action
- any management actions that could help facilitate completion of the action

Document Notes and Recommendations

Document Notes and Recommendations	All Phases, All Processes, All Steps
Activity Worksheets • Notes and Recommendations (Vol. 9)	*Reference Worksheets* • none

Background/Definitions

Notes – background information that you believe is relevant to record (i.e., information that you might want to refer to during a later activity)

Recommendations – ideas that you want to consider when you create mitigation plans or update your protection strategy during Process 5

Instructions

1. During the evaluation, you will likely think of notes or recommendations that you want to consider at a later time. Document each note or recommendation on the *Notes and Recommendations Worksheet* (Vol. 9).
2. Before you begin each process, review the notes and recommendations to reset context.

Phase 1: Build Asset-Based Threat Profiles

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

Table 1: Processes and Activities of Phase 1

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

Process S1: Identify Organizational Information

This process focuses on developing criteria for evaluating the impact of risks for the organization, identifying the organization's assets, and evaluating the organization's security practices.

S1.1 Establish Impact Evaluation Criteria

Activity S1.1: Establish Impact Evaluation Criteria	Phase 1, Process S1, Step 1
Activity Worksheets • Impact Evaluation Criteria (Vol. 4)	*Reference Worksheets* • none

Background/Definitions

Impact – the effect of a threat on an organization's mission and business objectives

Impact value – a qualitative measure of a specific risk's impact to the organization (high, medium, or low)

Impact evaluation criteria – a set of qualitative measures against which each risk's effect on an organization's mission and business objectives is evaluated. Impact evaluation criteria define ranges of high, medium, and low impacts for an organization.

Instructions

Step 1

1. Define a qualitative set of measures (impact evaluation criteria) against which you will be able to evaluate a risk's effect on your organization's mission and business objectives. Document your criteria on the *Impact Evaluation Criteria Worksheet* (Vol. 4). At a minimum, consider the following impact areas:
   - reputation/customer confidence
   - life/health of customers
   - fines/legal penalties
   - financial
   - productivity
   - other (e.g. Administrative actions such as audits and downsizing)

   Fill in any blanks in the criteria to make them meaningful to your organization. You can also change the words provided or add additional words as necessary.

   Note: Within each impact area, there is an option entitled "other" to insert a unique set of criteria. There is also an impact area entitled "other" available for new or unique impact areas.
2. Cross out any impact areas that do not apply to your organization on the *Impact Evaluation Criteria Worksheet* (Vol. 4).

S1.2 Identify Organizational Assets

Activity S1.2: Identify Organizational Assets	Phase 1, Process S1, Step 2

Activity Worksheets	*Reference Worksheets*
• Asset Identification (Vol. 4)	• none

Background/Definitions

Asset – something of value to the enterprise. Information technology assets are the combination of logical and physical assets and are grouped into specific classes (information, systems, services and applications, people).

Asset categories

- information – documented (paper or electronic) *data or intellectual property* used to meet the mission of an organization
- systems – a combination of information, software, and hardware assets that process and store *information*. Any host, client, or server can be considered a system.
- services and applications – software applications and services (operating systems, database applications, networking software, office applications, custom applications, etc.) that process, store, or transmit *information*
- people – the people in an organization who possess *unique skills, knowledge, and experience* that are difficult to replace

In an *information* security risk evaluation, assets should be linked to information in some way.

Instructions

Step 2

1. The first page of the *Asset Identification Worksheet* (Vol. 4) focuses on systems, information, and services and applications. Consider the following questions:
   - What systems do people in your organization need to perform their jobs?
   - What information do people in your organization need to perform their jobs?
   - What applications and services do people in your organization need to perform their jobs?
   - What other assets are closely related to these assets?

   Identify assets in your organization, and document them on the first page of the worksheet.

   Note: Each row in the worksheet contains assets that are related. In addition, you may record an asset in more than one row.

(continued on next page)

Guidelines

Activity S1.2: Identify Organizational Assets (cont.) Phase 1, Process S1, Step 2

Activity Worksheets	*Reference Worksheets*
• Asset Identification (Vol. 4)	• none

Instructions

Step 2 (cont.)

2. The third page of the *Asset Identification Worksheet* (Vol. 4) focuses on people. Consider the following questions:
   - Which people have a special skill or knowledge that is vital to your organization and would be difficult to replace?
   - What are their special skills or knowledge?
   - Which systems do these people use?
   - Which other assets do these people use (i.e., information, services, or applications)?

   Identify people assets in your organization, and document them on the third page of the worksheet.

   Note: You might find yourself iterating between these pages. Make sure that you are as complete as possible and that you document all *relevant* relationships among assets.

S1.3 Evaluate Organizational Security Practices

Activity S1.3: Evaluate Organizational Security Practices	Phase 1, Process S1, Steps 3-4
Activity Worksheets • Security Practices (Vol. 4)	*Reference Worksheets* • none

Background/Definitions

A security practice survey enables an analysis team to evaluate the extent to which security practices are reflected in the way its organization manages security.

Security practices – actions that help initiate, implement, and maintain security within an enterprise

Organizational vulnerabilities – weaknesses in organizational policy or practice that can result in unauthorized actions

Catalog of practices – a collection of good strategic and operational security practices that an organization can use to manage its security

Strategic practices – security practices that focus on organizational issues at the policy level. They include business-related issues as well as issues that require organization-wide plans and participation.

Operational practices – security practices that focus on technology-related issues. They include issues related to how people use, interact with, and protect technology on a day-to-day basis.

Stoplight status – how well an organization is performing in a security practice area. The following colors are assigned to an area based on perceived performance in that area:

- Green – The organization is performing the security practices in the area very well; there is no real need for improvement.
- Yellow – The organization is performing the security practices to some extent; there is room for improvement.
- Red – The organization is not performing the security practices in the area; there is significant room for improvement.

The following security practice areas are evaluated in OCTAVE-S.

Strategic Practice Areas	**Operational Practice Areas**
1. Security Awareness and Training	7. Physical Access Control
2. Security Strategy	8. Monitoring and Auditing Physical Security
3. Security Management	9. System and Network Management
4. Security Policies and Regulations	10. Monitoring and Auditing IT Security
5. Collaborative Security Management	11. Authentication and Authorization
6. Contingency Planning/Disaster Recovery	12. Vulnerability Management
	13. Encryption
	14. Security Architecture and Design
	15. Incident Management

(continued on next page)

Activity S1.3: Evaluate Organizational Security Practices (cont.)	Phase 1, Process S1, Steps 3-4
Activity Worksheets • Security Practices (Vol. 4)	*Reference Worksheets* • none

Instructions

Step 3a

Review the statements in each security practice area on the *Security Practices Worksheet* (Vol. 4) and answer the following question:

- To what extent is this statement reflected in your organization?

Circle the best response from the following options:

- *Very much* – The statement represents the current practice in the organization.
- *Somewhat* – The statement partially represents the current practice in the organization. Some aspects of the statement do not represent current practice in the organization.
- *Not at all* – The statement does not represent the current practice in the organization at all.

If you do not know whether a statement reflects security practice in your organization, do not circle any of the responses.

Step 3b

As you complete the survey questions, consider the following questions:

- What is your organization currently doing well in this area?
- What is your organization currently not doing well in this area?

The first question focuses on current security practices used by your organization, while the second centers on organizational vulnerabilities present in your organization.

Record examples of security practices and organizational vulnerabilities relevant to each security practice area.

Step 4

After completing Steps 3a and 3b, assign a stoplight status to each security practice area. The stoplight status should reflect how well you believe your organization is performing in each area. Use the following stoplight definitions as a guide:

- *Green* – The organization is performing the security practices in the area very well; there is no real need for improvement.
- *Yellow* – The organization is performing the security practices to some extent; there is room for improvement.
- *Red* – The organization is not performing the security practices in the area; there is significant room for improvement.

(continued on next page)

Activity S1.3: Evaluate Organizational Security Practices (cont.)	Phase 1, Process S1, Steps 3-4
Activity Worksheets • Security Practices (Vol. 4)	*Reference Worksheets* • none

Instructions (cont.)

Action Items, Notes, and Recommendations

1. Document all action items you identified during Process S1 on the *Action List Worksheet* (Vol. 9).

   Include the following information for each action item:

   - a description of the action
   - responsibility for completing the action
   - a date for completing the action
   - any management actions that could help facilitate completion of the action

2. Document notes relevant to the activities in Process S1 on the *Notes and Recommendations Worksheet* (Vol. 9).
3. Document all recommendations from Process S1 that you want to consider during Process S5 on the *Notes and Recommendations Worksheet* (Vol. 9).

Process S2: Create Threat Profiles

This process focuses on selecting critical assets from those previously identified, identifying security requirements for those assets, and identifying threats to those critical assets.

S2.1 Select Critical Assets

Activity S2.1: Select Critical Assets	Phase 1, Process S2, Steps 5-9

Activity Worksheets	*Reference Worksheets*
• Critical Asset Selection (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)	• Asset Identification (Vol. 4)

Background/Definitions

Critical assets – the most important assets to an organization. The organization will suffer a large adverse impact if

- a critical asset is disclosed to unauthorized people
- a critical asset is modified without authorization
- a critical asset is lost or destroyed
- access to a critical asset is interrupted

Instructions

Note: Before you begin Process S2, review any notes and recommendations that you recorded on the *Notes and Recommendations Worksheet*s (Vol. 4) during Process S1. These notes and recommendations could be relevant to the activities that you will conduct during Process S2.

Step 5

Review the assets that you recorded on the *Asset Identification Worksheet* (Vol. 4) and consider the following questions:

- Which assets would have a large adverse impact on the organization if one or more of the following occurred:
  - The asset or assets were disclosed to unauthorized people.
  - The asset or assets were modified without authorization.
  - The asset or assets were lost or destroyed.
  - Access to the asset or assets was interrupted.

As you consider the questions, think about the few information-related assets that are most essential to meeting the organization's mission or achieving its goals and objectives.

Record up to five critical assets on the *Critical Asset Selection Worksheet* (Vol. 4). Also record any relevant notes about each asset.

Note: Completing the "Notes" column is optional. Also, the numbers on the worksheet are not meant to indicate priority order.

(continued on next page)

Activity S2.1 Select Critical Assets (cont.) Phase 1, Process S2, Steps 5-9

Activity Worksheets	*Reference Worksheets*
• Critical Asset Selection (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)	• Asset Identification (Vol. 4)

Instructions (cont.)

Step 6

Start a *Critical Asset Workbook* (Vol. 5-8) for each critical asset.

Note: Each category of critical asset (systems, information, applications, people) has a unique Critical Asset Workbook (Vol. 5-8). The contents are similar for each Critical Asset Workbook, but the questions are worded slightly differently depending on asset category. Make sure that you select the appropriate volume for each critical asset.

Record the name of each critical asset on its *Critical Asset Information Worksheet* located in the appropriate Critical Asset Workbook (Vol. 5-8).

Step 7

Document your rationale for selecting each critical asset on that asset's *Critical Asset Information Worksheet* (Vol. 5-8).

Consider the following question:

- Why is this asset critical to the organization?

Step 8

Record a description for each critical asset on that asset's *Critical Asset Information Worksheet* (Vol. 5-8).

Consider the following questions:

- Who uses the asset?
- Who is responsible for the asset?

Step 9

Record assets that are related to each critical asset on that asset's *Critical Asset Information Worksheet* (Vol. 5-8). Refer to the *Asset Identification Worksheet* (Vol. 4) to determine which assets are related to each critical asset.

Consider the following question:

- Which assets are related to this asset?

S2.2 Identify Security Requirements for Critical Assets

Activity S2.2: Identify Security Requirements for Critical Assets	Phase 1, Process S2, Steps 10-11

Activity Worksheets	*Reference Worksheets*
• Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)	• none

Background/Definitions

Security requirements – statements describing the qualities of information-related assets that are important to an organization. Typical security requirements are confidentiality, integrity, and availability.

Confidentiality – the need to keep proprietary, sensitive, or personal information private and inaccessible to anyone who is not authorized to see it

Integrity – the authenticity, accuracy, and completeness of an asset

Availability – when or how often an asset must be present or ready for use

Note: Security requirements within OCTAVE-S focus on what the requirements should be for an asset, not what they currently are.

Instructions

Step 10

1. Record the security requirements for each critical asset on that asset's *Critical Asset Information Worksheet* (Vol. 5-8).

   Note: Security requirements focus on what the requirements *should* be for an asset, not what they currently are.

   Consider the following question:

   - What are the security requirements for this asset?

   A statement for each category of security requirements is presented on the *Critical Asset Information Worksheet* (Vol. 5-8). If a category is applicable for a critical asset, mark an 'X' in the box next to that category.

2. Complete the security requirement for each applicable category for a critical asset. At a minimum, fill in the blanks provided.

   You can change the words provided or add additional words as necessary.

   Note: A category entitled "other" is provided for additional security requirements that do not fall into the categories of confidentiality, integrity, and availability.

Step 11

For each critical asset, record the most important security requirement on that asset's *Critical Asset Information Worksheet* (Vol. 5-8) by marking an 'X' in the box next to the category of security requirements that is most important for that asset.

Consider the following question:

- Which security requirement is most important for this asset?

S2.3 Identify Threats to Critical Assets

Activity S2.3: Identify Threats to Critical Assets	Phase 1, Process S2, Steps 12-16
Activity Worksheets • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • Threat Translation Guide in appropriate Critical Asset Workbook (Vol. 5-8)

Background/Definitions

Threat – an indication of a potential undesirable event. A threat refers to a situation in which a person could do something undesirable (an attacker initiating a denial-of-service attack against an organization's email server) or a natural occurrence could cause an undesirable outcome (a fire damaging an organization's information technology hardware).

Threat profile – a structured way of presenting a range of threats to a critical asset. Threats in the profile are grouped according to the source of the threat.

Generic threat profile – a catalog of threats that contains a range of all potential threats under consideration. The generic threat profile is a starting point for creating a unique threat profile for each critical asset.

Threats are represented using the following properties:

- Asset – something of value to the enterprise
- Access – how the asset is accessed by an actor (network access, physical access). Access applies only to human actors.
- Actor – who or what may violate the security requirements (confidentiality, integrity, availability) of an asset
- Motive – the intent of an actor (e.g., deliberate or accidental). Motive applies only to human actors.
- Outcome – the immediate result (disclosure, modification, destruction, loss, interruption) of violating the security requirements of an asset

In OCTAVE-S, threats are represented visually in a tree structure, often referred to as a threat tree. There is one threat tree for each of the following categories of threat source:

Category	**Definition**
Human actors using network access	The threats in this category are network-based threats to an organization's critical assets. They require direct action by a person and can be deliberate or accidental in nature.
Human actors using physical access	The threats in this category are physical threats to an organization's critical assets. They require direct action by a person and can be deliberate or accidental in nature.
System problems	The threats in this category are problems with an organization's information technology systems. Examples include hardware defects, software defects, malicious code (e.g., viruses), and other system-related problems.
Other problems	The threats in this category are problems or situations that are outside the control of an organization. This category of threats includes natural disasters (e.g., floods, earthquakes) and interdependency risks. Interdependency risks include the unavailability of critical infrastructures (e.g., power supply).

(continued on next page)

Activity S2.3: Identify Threats to Critical Assets (cont.) Phase 1, Process S2, Steps 12-16

Activity Worksheets	*Reference Worksheets*
• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	• Threat Translation Guide in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions

Note: Each category of critical asset (systems, information, applications, people) has a unique *Risk Profile Worksheet*. You will find it in the Critical Asset Workbook (Vol. 5-8) for that asset category.

Note: You will complete only selected parts of the *Risk Profile Worksheet* (Steps 12-16) during this activity. You will complete the remaining parts (Steps 22, 24, 26, and 27) later in the evaluation.

Step 12

Note: If you have difficulty interpreting a threat on any threat tree, review the description and examples of that threat in the *Threat Translation Guide* (Vol. 5-8).

1. Select the appropriate worksheet for each critical asset.

   Note: The following four trees apply to systems, information, and services and applications:

   - human actors using network access
   - human actors using physical access
   - system problems
   - other problems

   Note: Only one tree applies to people: other problems.

2. Complete all appropriate threat trees for each critical asset. When marking a threat tree, consider the following questions:

   - For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.
   - For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

   Note: Make sure to mark a threat if there is even a remote possibility that a threat could occur. You will have the opportunity to accept the threat later in the evaluation. Right now, you should look at the widest range of possible threats.

(continued on next page)

Activity S2.3: Identify Threats to Critical Assets (cont.) Phase 1, Process S2, Steps 12-16

Activity Worksheets	*Reference Worksheets*
• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	• Threat Translation Guide in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 13

Note: You complete this step only for the following categories of threat:

- human actors using network access
- human actors using physical access

In this step, you provide additional details about the following actor-motive combinations:

- insiders acting accidentally
- insiders acting deliberately
- outsiders acting accidentally
- outsiders acting deliberately

1. As you complete threat trees for human actors using network access, consider the following question:

   - Which actors pose the biggest threats to this asset via the network?

   Record specific examples of threat actors on the *Risk Profile Worksheet* (Vol. 5-8) for each applicable actor-motive combination.

2. As you complete threat trees for human actors using physical access, consider the following question:

   - Which actors pose the biggest threats to this asset via physical means?

   Record specific examples of threat actors on the *Risk Profile Worksheet* (Vol. 5-8) for each applicable actor-motive combination.

(continued on next page)

Activity S2.3: Identify Threats to Critical Assets (cont.) Phase 1, Process S2, Steps 12-16

Activity Worksheets	*Reference Worksheets*
• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	• Threat Translation Guide in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 14

Note: You complete this step only for the following categories of threat:

- human actors using network access
- human actors using physical access

In this step, you provide additional details about the following actor-motive combinations:

- insiders acting deliberately
- outsiders acting deliberately

1. Consider the following question for both actor-motive combinations:
   - How strong is the actor's motive?

   You are estimating highest motive strength based on the specific actors you identified during Step 13.

   Mark an 'X' in the box next to the best response from the following options:

   - *High* – The actor is focused on attacking your organization, has very defined goals, is specifically targeting the critical asset, will apply extraordinary means to attack the critical asset, and will go to extraordinary lengths to ensure success.
   - *Medium*– The actor is focused on attacking your organization, has general goals, is targeting a range of assets in your organization, has limits on the means that will be applied to attack the critical asset, and has an explicit or implicit exit strategy defining when to abandon the attack.
   - *Low*– The actor is focused on attacking an organization (not necessarily yours), does not have specific goals, is targeting any asset that can be attacked easily, will apply limited means to the attack, and will quickly abandon the attack if success doesn't prove to be easy.

(continued on next page)

Activity S2.3: Identify Threats to Critical Assets (cont.)	Phase 1, Process S2, Steps 12-16

Activity Worksheets	*Reference Worksheets*
• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	• Threat Translation Guide in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 14 (cont.)

2. Consider the following question for each estimate of motive strength:

    - How confident are you in this estimate?

    Mark an 'X' in the box next to the best response from the following options:

    - *Very* – You have a considerable amount of objective data related to your estimate. Any reasonable person reviewing the objective data would reach the same conclusion.
    - *Somewhat* – You have a limited amount of objective data related to your estimate. A reasonable person would need to make key inferences and assumptions to reach the same conclusion. However it is likely that a reasonable person would arrive at the same conclusion.
    - *Not at all* – You have little or no objective data related to your estimate. A reasonable person could arrive at a different conclusion because there are little or no objective data upon which to base the estimate.

Step 15

Note: Complete this step for all categories of threat.

1. Consider the following question for each active threat:

    - How often has this threat occurred in the past?

    Review any objective data that you might have (e.g., logs, incident data) as well as subjective data (what people on the analysis team or people in your organization recall). Fill in the blanks in the following statement for each threat:

    - _____ times in _____ years

(continued on next page)

Activity S2.3: Identify Threats to Critical Assets (cont.) Phase 1, Process S2, Steps 12-16

Activity Worksheets	*Reference Worksheets*
• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	• Threat Translation Guide in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 15 (cont.)

2. Consider the following question for each estimate of threat history:

   - How accurate are the data?

   Mark an 'X' in the box next to the best response from the following options:

   - *Very* – You have a considerable amount of objective data related to your estimate. Any reasonable person reviewing the objective data would reach the same conclusion.
   - *Somewhat* – You have a limited amount of objective data related to your estimate. A reasonable person would need to make key inferences and assumptions to reach the same conclusion. However it is likely that a reasonable person would arrive at the same conclusion.
   - *Not at all* – You have little or no objective data related to your estimate. A reasonable person could arrive at a different conclusion because there are little or no objective data upon which to base the estimate.

Step 16

This step provides additional context where appropriate. Give examples, or scenarios, of how specific threats could affect the critical asset. Record additional context and areas of concern for each source of threat.

Action Items, Notes, and Recommendations

1. Document all action items that you identified during Process S2 on the *Action List Worksheet* (Vol. 9).

   Include the following information for each action item:

   - a description of the action
   - responsibility for completing the action
   - a date for completing the action
   - any management actions that could help facilitate completion of the action

2. Document notes relevant to the activities in Process S2 on the *Notes and Recommendations Worksheet* (Vol. 9).
3. Document all recommendations from Process S2 that you want to consider during Process S5 on the *Notes and Recommendations Worksheet* (Vol. 9).

Phase 2: Identify Infrastructure Vulnerabilities

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

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

Table 2: Processes and Activities of Phase 2

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

Process S3: Examine the Computing Infrastructure in Relation to Critical Assets

This process focuses on examining access paths in the infrastructure for the critical assets and then analyzing the technology-related processes associated with the infrastructure.

S3.1 Examine Access Paths

Activity S3.1: Examine Access Paths	Phase 2, Process S3, Steps 17-18
Activity Worksheets • Network Access Paths in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Background/Definitions

Network access paths – ways in which systems, devices, information, or services can be accessed via an organization's network

System of interest – the system or systems that are most closely linked to a critical asset, for example:

- the system where the asset "lives"
- the system where you would go to get an "official" copy of the asset
- the system that gives legitimate users access to a critical asset
- the system that gives a threat actor access to a critical asset

Key classes of components – categories of devices and networks used to access a system of interest. These devices and networks are either part of or related to a system of interest. When legitimate users access a critical asset, they access components from these classes. Threat actors also access components from these classes when the actors deliberately target a critical asset.

Access points – interfaces that directly or indirectly allow access to a system of interest. These interfaces are grouped according to the following categories:

- components of the system of interest
- system access by people
- intermediate access points
- other interfaces and data storage locations
- other systems

System access by people – types of components that people (e.g., users, attackers) use to access a system of interest. These components constitute access points that can originate internally or externally to an organization's systems and networks.

Intermediate access points – networks used to transmit information and applications from the system of interest to people

Data storage locations – additional types of components used to store critical information or provide data support services related to a system of interest (e.g., storage devices used to back up information stored on a system of interest)

Other systems and components – systems that access critical information or services from a system of interest; also, other classes of components that can be used to access critical information or applications from the system of interest

(continued on next page)

Activity S3.1: Examine Access Paths (cont.) Phase 2, Process S3, Steps 17-18

Activity Worksheets	*Reference Worksheets*
• Network Access Paths in appropriate Critical Asset Workbook (Vol. 5-8)	• Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Background/Definitions (cont.)

The standard classes of components considered in OCTAVE-S are described in the table below:

Component Class	Description
Servers	hosts within your information technology infrastructure that provide information technology services to your organization
Internal networks	interconnectivity that links computers and systems. Internal networks are maintained by people within your organization
On-site workstations	hosts on your networks that staff members use to conduct business
Laptops	portable PCs that staff members use to access information remotely via your organization's networks
PDA/wireless components	Devices (such as PDAs, cell phones, and wireless access points) that staff members may use to access information (e.g., email)
Other systems	systems, processes, and/or applications that access critical information or services from a system of interest. Items in this category link to or use content from the system of interest in some manner.
Storage devices	devices where information is stored, often for backup purposes
External networks	interconnectivity that links computers and systems. External networks are not part of your organization's networks (e.g., the Internet) or are managed for your organization by an external organization.
Home/external workstations	devices that staff members and individuals outside of your organization use to access information remotely via your organization's networks
Others	any other type of device that could be part of your threat scenarios, but does not fall into the above classes

(continued on next page)

Activity S3.1: Examine Access Paths (cont.) Phase 2, Process S3, Steps 17-18

Activity Worksheets	*Reference Worksheets*
• Network Access Paths in appropriate Critical Asset Workbook (Vol. 5-8)	• Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions

Note: Before you begin Process S3, review any notes and recommendations that you recorded on the *Notes and Recommendations Worksheet* (Vol. 9) during previous processes. These notes and recommendations could be relevant to the activities that you will conduct during Process S3.

Complete the steps in this activity for each critical asset that is subject to network-based threats.

OCTAVE-S requires you to perform a cursory examination of how you access critical assets via your organization's networks as well as the extent to which security is considered when configuring and maintaining your organization's computers and networks. If you find that your analysis team is unable to perform Activity S3.1, the members of the team might not possess the necessary skills for the activity and you may need to augment the team's skill set for Activity S3.1. If you do not have anyone within your organization with the appropriate skills for the activity, record a note indicating that the organization lacks people with a basic understanding of computer networking on the *Notes and Recommendations Worksheet* (Vol. 9). If appropriate, you can also record a recommendation for addressing the situation.

Step 17

First, you need to establish the system(s) that is most closely linked to a critical asset. You should think about where the asset "lives," where you would go to get an "official" copy of the asset, the system that gives legitimate users access to a critical asset, and the systems that a threat actor would target to access a critical asset.

Consider the following question:

- Which system or systems are most closely linked to the critical asset? On which system(s) is the critical asset stored and processed?

You could identify multiple systems of interest for a critical asset. Try to narrow the list to the "official" source for the asset.

Record the name(s) of the system(s) of interest on the *Network Access Paths Worksheet* (Vol. 5-8).

Note: If you are analyzing a systems asset, the system of interest is the system itself.

(continued on next page)

Activity S3.1: Examine Access Paths (cont.) Phase 2, Process S3, Steps 17-18

Activity Worksheets	*Reference Worksheets*
• Network Access Paths in appropriate Critical Asset Workbook (Vol. 5-8)	• Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 18a

1. When you examine access paths, you first establish which components are part of the system of interest. Consider the following question:

   - Which of the following classes of components is part of the system of interest?

   After considering the question, mark an 'X' in each box next to each appropriate response in the "System of Interest" area on the *Network Access Paths Worksheet* (Vol. 5-8). You are presented with the following options:

   - servers
   - internal networks
   - on-site workstations
   - others

   If you select "others," be sure to list specific classes of components.

2. When you select a key class of components, document any relevant subclasses or cite specific examples when appropriate. For example, if you select "on-site workstations," you might find it necessary to further refine the designation based on classes of users. Thus, if workstations are configured differently based on how they are used, you could determine that "on-site workstations" includes two subclasses of workstations: staff and management.

(continued on next page)

Activity S3.1: Examine Access Paths (cont.) Phase 2, Process S3, Steps 17-18

Activity Worksheets	*Reference Worksheets*
• Network Access Paths in appropriate Critical Asset Workbook (Vol. 5-8)	• Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 18b

1. Determine how information and applications from the system of interest is transmitted to people who access that system. Consider the following question:
   - Which types of components are used to transmit information and applications from the system of interest to people?

   Note: You might decide that you need to first review the types of components used by people to access the system of interest (Step 18c) before completing this step.

   After considering the questions, mark an 'X' in each box next to each appropriate response in the "Intermediate Access Points" area on the *Network Access Paths Worksheet* (Vol. 5-8). You are presented with the following options:
   - internal networks
   - external networks
   - others

   If you select "others," be sure to list specific classes of components.
2. When you select a key class of components, document any relevant subclasses or cite specific examples when appropriate. For example, if you select "internal networks," you might find it necessary to further refine the designation if your organization maintains multiple networks. Thus, you could determine that you need to account for two subclasses of internal networks: network A and network B.

(continued on next page)

Activity S3.1: Examine Access Paths (cont.) Phase 2, Process S3, Steps 17-18

Activity Worksheets	*Reference Worksheets*
• Network Access Paths in appropriate Critical Asset Workbook (Vol. 5-8)	• Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 18c

1. Examine which components *people use* to access the system of interest. Consider the following question:

   - From which types of components can people (e.g., users, attackers) access the system of interest?

   As you review how people can access the system of interest, think about access points both internal and external to your organization's networks.

   After considering the question, mark an 'X' in each box next to each appropriate response in the "System Access by People" column area on the *Network Access Paths Worksheet* (Vol. 5-8). You are presented with the following options:

   - on-site workstations
   - laptops
   - PDAs/wireless components
   - home/external workstations
   - others

   If you select "others," be sure to list specific classes of components.

2. When you select a key class of components, document any relevant subclasses or cite specific examples when appropriate. For example, if you select "on-site workstations," you might find it necessary to further refine the designation based on classes of users. Thus, if workstations are configured differently based on how they are used, you could determine that "on-site workstations" includes two subclasses of workstations: staff and management.

(continued on next page)

Activity S3.1: Examine Access Paths (cont.)	Phase 2, Process S3, Steps 17-18
Activity Worksheets • Network Access Path in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 18d

1. Determine if any data storage locations are linked to information on the system of interest. Consider the following question:

   - On which classes of components is information from the system of interest stored for backup purposes?

   After considering the questions, mark an 'X' in each box next to each appropriate response in the "Data Storage Locations" area on the *Network Access Paths Worksheet* (Vol. 5-8). You are presented with the following options:

   - storage devices
   - others

   If you select "others," be sure to list specific classes of components.

2. When you select a key class of components, document any relevant subclasses or cite specific examples when appropriate. For example, if you select "storage devices," you might find it necessary to further refine the designation based on where different types of information are backed up. Thus, you could determine that "storage devices" includes two subclasses of workstations: accounting backups and personnel information backups.

Step 18e

Finally, examine other systems and components that access information, services, or applications from the system of interest. Consider the following questions:

- Which other systems access information or applications from the system of interest?
- Which other classes of components can be used to access critical information or applications from the system of interest?

After considering the question, record the names of applicable systems or components in the blanks provided in the "Other Systems and Components" area on the *Network Access Paths Worksheet* (Vol. 5-8). Mark an 'X' in each box next to a filled-in blank.

S3.2 Analyze Technology-Related Processes

Activity S3.2: Analyze Technology-Related Processes	Phase 2, Process S3, Steps 19-21
Activity Worksheets • Infrastructure Review (Vol. 4)	*Reference Worksheets* • Network Access Path in Critical Asset Workbook (Vol. 5-8)

Background/Definitions

The analysis focus shifts during Activity S3.2. During Activity S2.3, you performed analysis activities from an asset perspective when you identified threats to critical assets. Likewise, during Activity S3.1, you performed analysis activities from an asset perspective when you examined access paths in relation to critical assets.

However, during Activity S3.2, rather than performing analysis activities from an asset perspective, you now assume an infrastructure perspective. During this activity, you analyze the technology-related processes used when configuring and maintaining the computing infrastructure.

During Activity S3.2, you compile information for each class of component that you identified during the previous activity. The information for each class includes

- the critical assets that are related to each class
- the party (or parties) responsible for maintaining and securing each class of components
- the extent to which security is considered when configuring and maintaining each class of components (very much, somewhat, not at all, don't know)
- how you determined the extent to which security is considered when configuring and maintaining each class of components (formal techniques, informal means, other)
- any additional information, notes, and issues you want to record for each class

(continued on next page)

Activity S3.2: Analyze Technology-Related Processes (cont.)	Phase 2, Process S3, Steps 19-21
Activity Worksheets • Infrastructure Review (Vol. 4)	*Reference Worksheets* • Network Access Path in Critical Asset Workbook (Vol. 5-8)

Instructions

Step 19a

1. Review the classes of components you identified for each critical asset during Activity S3.1 on that asset's *Network Access Paths Worksheet* (Vol. 5-8). In this step, you simply mark the path to each class you selected in Steps 18a-18e. Consider the following question:

   - Which classes of components are related to one or more critical assets?

   For each class that is related to one or more critical asset, mark that path on the *Infrastructure Review Worksheet* (Vol. 4).

2. Recall that during Steps 18a-18e, you also documented relevant subclasses or cited specific examples for each class when appropriate. For example, when you selected "on-site workstations," you might have found it necessary to further refine the designation based on classes of users. Thus, if workstations are configured differently based on how they are used, you might have determined that "on-site workstations" includes two subclasses of workstations related to a critical asset: staff and management. As you looked at other critical assets, you might have identified additional subclasses.

   Document any relevant subclasses or specific examples for each class, when appropriate, in the space provided on the *Infrastructure Review Worksheet* (Vol. 4). If you have identified no subclasses or examples for a given class, you can record "all" under that class to denote that there are no variations or subclasses for that particular class of components.

Step 19b

1. Now you are going to note which critical assets are related to each class of components. For example, during the previous activity, you might have noted that "on-site workstations" were part of or related to the systems of interest for three critical assets. In this step, you document that information.

   First, you need to transcribe the name of each critical asset to the *Infrastructure Review Worksheet* (Vol. 4). At the top of *Infrastructure Review Worksheet* (under Step 19b) is an area that is numbered from 1 through 5. This is the space where you should record the names of your organization's critical assets. Document the name of each critical asset in the spaces provided.

2. Consider the following question:

   - Which critical assets are related to each class of components?

   Refer to the *Network Access Paths Worksheets* (Vol. 5-8) for each critical asset and review the information recorded under Steps 18a-18e. For each class you marked on the *Infrastructure Review Worksheet* (Vol. 4) during Step 19a, record which critical assets are related to that class by marking an 'X' in the boxes below the applicable asset names. If you identified specific subclasses for a class of component, be sure to denote which subclasses are related to which critical assets.

(continued on next page)

Activity S3.2: Analyze Technology-Related Processes (cont.)	Phase 2, Process S3, Steps 19-21
Activity Worksheets • Infrastructure Review (Vol. 4)	*Reference Worksheets* • Network Access Path in Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 20

Next, identify the party (or parties) responsible for maintaining and securing each class of components. If you identified more than one subclass for any given class of components, you must identify the party (or parties) responsible for maintaining and securing each subclass.

For each class you marked on the *Infrastructure Review Worksheet* (Vol. 4) during Step 19a, consider the following question:

- Who is responsible for maintaining and securing each class of component?

Record the name of the party or parties responsible for maintaining and securing each class (or subclass when applicable) of component on the *Infrastructure Review Worksheet* (Vol. 4).

Step 21

1. Determine how well you believe each class of components is currently being protected. If you identified more than one subclass for any given class of components, you must determine how well you believe each subclass is currently being protected. There could be variations in how subclasses within the same class are protected, especially if a different party is responsible for configuring and maintaining each subclass.

   Consider the following question:

   - To what extent is security considered when configuring and maintaining each class of components?

   Based on your answer to the question, mark an 'X' on the scale at the point that indicates how much security is considered when configuring and maintaining each class of components. The following points are provided on the *Infrastructure Review Worksheet* (Vol. 4) as references on the scale:

   - *Very much* – You have a considerable amount of objective data related to your estimate. Any reasonable person reviewing the objective data would reach the same conclusion.
   - *Somewhat* – You have a limited amount of objective data related to your estimate. A reasonable person would need to make key inferences and assumptions to reach the same conclusion. However it is likely that a reasonable person would arrive at the same conclusion.
   - *Not at all* – You have little or no objective data related to your estimate. A reasonable person could arrive at a different conclusion because there are little or no objective data upon which to base the estimate.
   - *Don't Know* – You do not have enough experience and expertise to make a plausible guess.

(continued on next page)

Activity S3.2: Analyze Technology-Related Processes (cont.) Phase 2, Process S3, Steps 19-21

Activity Worksheets	*Reference Worksheets*
• Infrastructure Review (Vol. 4)	• Network Access Path in Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 21(cont.)

2. You should also specifically note the sources for any data you used when determining the extent to which security is considered when configuring and maintaining each class of components.

   Consider the following question:

   - How do you know?

   Mark an 'X' in the box next to the best response to the above question from the following options on the *Infrastructure Review Worksheet* (Vol. 4):

   - *Formal Techniques* – You employed rigorous data gathering and analysis techniques to reach your conclusion. This can include a targeted vulnerability evaluation of the computing infrastructure by experienced personnel, a formal audit of components by qualified personnel, or any other formal evaluation/analysis technique. Provide any additional information in the "Notes/Issues" column when appropriate.
   - *Informal Means* – You performed a cursory evaluation of the situation to reach your conclusion. This can include a very limited vulnerability evaluation of the computing infrastructure, a limited review or audit of components, or any other incomplete or ad hoc technique. This can also include any rigorous data gathering and analysis techniques performed by inexperienced personnel. Provide any additional information in the "Notes/Issues" column when appropriate.
   - Other – Use this category to identify any other means you used to reach your conclusion that does not fall into either of the above categories. Provide any additional information in the "Notes/Issues" column when appropriate.

   Also document any other relevant notes or issues related to a component class in the space provided on the *Infrastructure Review Worksheet* (Vol. 4) when appropriate.

(continued on next page)

Activity S3.2: Analyze Technology-Related Processes (cont.)	Phase 2, Process S3, Steps 19-21
Activity Worksheets • Infrastructure Review (Vol. 4)	*Reference Worksheets* • Network Access Path in Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Gap Analysis

Refine Phase 1 information based on the analysis of access paths and technology-related processes. Perform the following tasks:

- Update the *Risk Profile Worksheet* (Vol. 5-8) for each critical asset when appropriate. Mark any additional branches of the threat trees if your Phase 2 analysis warrants it (Step 12). Document any additional context for each new branch you mark (Steps 13-16). Also look for instances where you can revise existing areas of concern by adding additional details, or where you can identify new areas of concern (Step 16).
- Update the *Security Practices Worksheet* (Vol. 4) when appropriate. Revise your responses to the survey questions if your Phase 2 analysis warrants it. Also look for instances where you can revise existing security practices and organizational vulnerabilities by adding additional details, or where you can identify new security practices and organizational vulnerabilities. Finally, review the information for each security practice area for which you have made additions or changes, and revise the stoplight status for that area when appropriate.

Action Items, Notes, and Recommendations

1. Document all action items you identified during Process S3 on the *Action List Worksheet* (Vol. 9).

   Include the following information for each action item:

   - a description of the action
   - responsibility for completing the action
   - a date for completing the action
   - any management actions that could help facilitate completion of the action

2. Document notes relevant to the activities in Process S3 on the *Notes and Recommendations Worksheet* (Vol. 9).
3. Document all recommendations from Process S3 that you want to consider during Process S5 on the *Notes and Recommendations Worksheet* (Vol. 9).

Phase 3: Develop Security Strategy and Plans

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

Table 3: Processes and Activities of Phase 3

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

Process S4: Identify and Analyze Risks

This process focuses on evaluating the impact and probability of threats to critical assets and establishing probability evaluation criteria.

S4.1 Evaluate Impacts of Threats

Activity S4.1: Evaluate Impacts of Threats	Phase 3, Process S4, Step 22
Activity Worksheets • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • Impact Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Background/Definitions

Risk – the possibility of suffering harm or loss. Risk refers to a situation where a person could do something undesirable or a natural occurrence could cause an undesirable outcome, resulting in a negative impact or consequence.

A risk is composed of

- an event
- uncertainty
- a consequence

In information security, the basic event is a threat.

Uncertainty is embodied in much of the information gathered during the OCTAVE-S evaluation. There is uncertainty surrounding whether a threat will occur and whether the organization is sufficiently protected against the threat actor. Uncertainty is often represented using likelihood of occurrence, or probability.

The consequence that ultimately matters in information security risk is the resulting impact on the organization due to a threat. Impact describes how an organization might be affected based on the following threat outcomes:

- disclosure of a critical asset
- modification of a critical asset
- loss/destruction of a critical asset
- interruption of a critical asset

The outcomes listed above are directly related to assets; they describe the effect of threats on assets. Impact is focused on the organization; it is the direct link back to the organization's mission and business objectives.

In Activity S1.1, impact evaluation criteria were created for the following impact areas:

- reputation/customer confidence
- life/health of customers
- fines/legal penalties
- financial
- productivity
- other

(continued on next page)

Activity S4.1: Evaluate Impacts of Threats (cont.) Phase 3, Process S4, Step 22

Activity Worksheets	*Reference Worksheets*
• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	• Impact Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions

Note: Before you begin Process S4, review any notes and recommendations you recorded on the *Notes and Recommendations Worksheet* (Vol. 9) during previous processes. These notes and recommendations could be relevant to the activities you will conduct during Process S4.

Step 22

Note: Before evaluating potential impacts on the organization resulting from threats to critical assets, you should review critical asset and threat information that you documented previously during the evaluation.

1. Review the threat information you recorded on the *Risk Profile Worksheet* (Vol. 5-8) for each critical asset. Focus on the following items:
   - threats to the critical assets
   - threat context (threat actors, motive, history)
   - additional threat context
2. Review the information you recorded on each *Critical Asset Worksheet* (Vol. 5-8). Focus on the following items:
   - rationale for selecting related assets
   - security requirements
   - most important security requirement
3. Review the information you recorded on the *Impact Evaluation Criteria Worksheet* (Vol. 4). Focus on how you defined high, medium, and low impacts for your organization.

   Use the impact evaluation criteria to evaluate each threat's impact on your organization's mission and business objectives. Be sure to review the criteria you recorded for the following areas:
   - reputation/customer confidence
   - life/health of customers
   - fines/legal penalties
   - financial
   - productivity
   - other

(continued on next page)

Activity S4.1: Evaluate Impacts of Threats (cont.)	Phase 3, Process S4, Step 22
Activity Worksheets • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	*Reference Worksheets* • Impact Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 22 (cont.)

4. For each critical asset, consider the following questions for each threat to that asset:
    - What is the potential impact to the organization's reputation?
    - What is the potential impact on customer confidence?
    - What is the potential impact to customers' health or safety?
    - What is the potential impact to staff members' health or safety?
    - What fines or legal penalties could be imposed on the organization?
    - What is the potential financial impact to the organization?
    - What is the potential impact to the organization's or customers' productivity?
    - What other impacts could occur?

    As you review the questions, think about the potential impact on your organization due to each active threat.

    Note: Each of the above questions is linked to an impact area.

5. After reviewing the above questions, compare the potential impacts you discussed for each impact area against the impact evaluation criteria for that area.

    Using the impact evaluation criteria as a guide, assign an impact measure (high, medium, or low) for each active threat.

    Document each impact on the *Risk Profile Worksheet* (Vol. 5-8) by recording
    - "H" for each high impact
    - "M" for each medium impact
    - "L" for each low impact

    Note: You might identify multiple impacts for a given threat, which could lead to more than one impact value for a given impact area. If this happens, record the highest value for that impact area on the *Risk Profile Worksheet* (Vol. 5-8).

S4.2 Establish Probability Evaluation Criteria

Activity S4.2: Establish Probability Evaluation Criteria	Phase 3, Process S4, Step 23
Activity Worksheets • Probability Evaluation Criteria (Vol. 4)	*Reference Worksheets* • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)

Background/Definitions

Probability – the likelihood that an event will occur

Probability value – a qualitative measure of a threat's probability (high, medium, or low)

Probability evaluation criteria – a set of qualitative measures used to estimate the likelihood of a threat's occurrence. Probability evaluation criteria define frequency ranges for high, medium, and low probabilities; they indicate how often threats occur over a common period of time.

Time between events – an estimate of how frequently an event might occur (e.g., weekly, once every two years)

Annualized frequency – the projected likelihood of a threat's occurrence in a given year

Information security threat probabilities are estimated using a combination of objective data, subjective experience, and expertise. If you are using OCTAVE-S for the first time, you likely lack objective data related to threats. You also might lack experience and expertise in information security and/or risk management. ***For this reason, probability is considered to be optional in OCTAVE-S.*** Each team needs to decide whether to use probability as well as how to use it.

In OCTAVE-S, probability values are defined by a set of evaluation criteria that are categorized according to frequency of occurrence. Probability evaluation criteria define a standard set of definitions for probability values. These criteria define high, medium, and low measures of threat probabilities.

Probability measures are defined by considering a range of frequencies (i.e., the likelihood of a threat's occurrence in a given year):

- daily
- weekly
- monthly
- 4 times per year
- 2 times per year
- once per year
- once every 2 years
- once every 5 years
- once every 10 years
- once every 20 years
- once every 50 years

(continued on next page)

Activity S4.2: Establish Probability Evaluation Criteria (cont.) Phase 3, Process S4, Step 23

Activity Worksheets	*Reference Worksheets*
• Probability Evaluation Criteria (Vol. 4)	• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 23 (optional)

1. Your goal is to define probability measures based on how often threats are likely to occur.

   Review the following information from the *Risk Profile Worksheet* (Vol. 5-8):

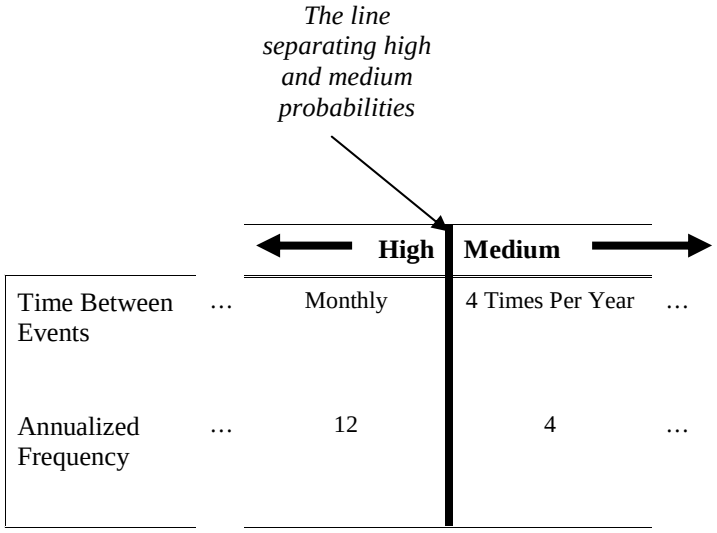
   - the types of threats to critical assets
   - how often each threat has occurred in the past (history)
   - any additional relevant information you recorded

2. Consider the following questions:

   - What defines a "high" likelihood of occurrence? How often must a threat occur to be considered a high-probability threat?
   - What defines a "medium" likelihood of occurrence? How often must a threat occur to be considered a medium-probability threat?
   - What defines a "low" likelihood of occurrence? How often must a threat occur to be considered a low-probability threat?

3. On the *Probability Evaluation Criteria Worksheet* (Vol. 4), draw vertical lines that separate high from medium probabilities and medium from low probabilities.

   Be sure to synchronize the boundaries between levels of probability. For example, when drawing the distinction between high and medium probabilities, you might draw a vertical line between monthly events and events that occur four times a year. This is illustrated in the diagram below.



(continued on next page)

Activity S4.2: Establish Probability Evaluation Criteria (cont.) Phase 3, Process S4, Step 23

Activity Worksheets	*Reference Worksheets*
• Probability Evaluation Criteria (Vol. 4)	• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 23 (cont.)

What if an event occurs six times a year? Should that threat be assigned a high or medium probability? You need to make sure that your criteria have no such gaps. In this case, you could

A. Change the boundary for medium probability threats to "less than monthly" (i.e., <12). This is shown below.

The boundary for medium probabilities has been changed

		High	Medium	
Time Between Events	…	Monthly	~~4 Times Per Year~~ *Less Than Monthly*	…
Annualized Frequency	…	12	~~4~~ *<12*	…

B. Change the boundary for high-probability threats to "greater than four times a year" (i.e., >4).

The boundary for high probabilities has been changed

		High	Medium	
Time Between Events	…	~~Monthly~~ *Greater Than 4 Times Per Year*	4 Times Per Year	…
Annualized Frequency	…	~~12~~ *>4*	~~4~~	…

(continued on next page)

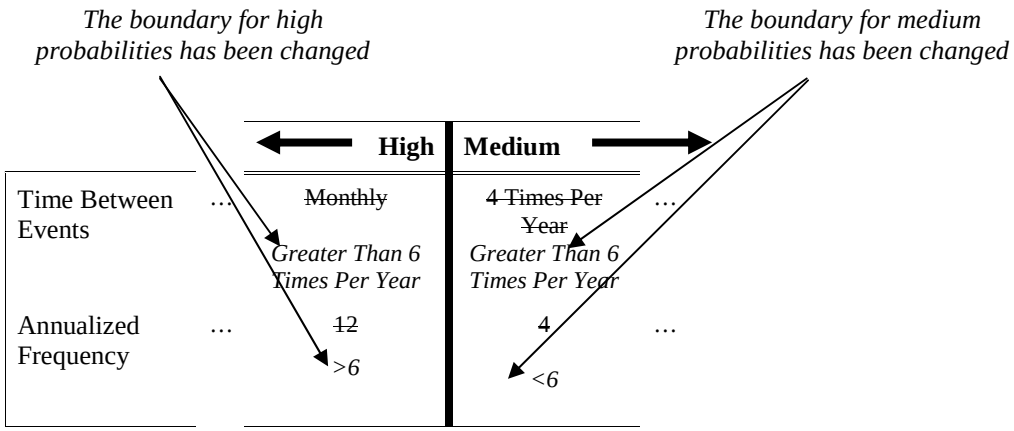
Activity S4.2: Establish Probability Evaluation Criteria (cont.) Phase 3, Process S4, Step 23

Activity Worksheets	*Reference Worksheets*
• Probability Evaluation Criteria (Vol. 4)	• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 23 (cont.)

C. Change the boundaries for both high- and medium-probability threats. The boundary for high-probability threats could be changed to "six times a year," while the boundary for medium-probability threats could be "less than six times a year." This is shown below.



The key is to ensure that there are no gaps between your definitions of "high" and "medium" measures of probability and between your definitions of "medium" and "low" measures of probability.

S4.3 Evaluate Probabilities of Threats

Activity S4.3: Evaluate Probabilities of Threats Phase 3, Process S4, Step 24

Activity Worksheets	*Reference Worksheets*
• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	• Probability Evaluation Criteria (Vol. 4)

Background/Definitions

A risk is composed of

- an event
- uncertainty
- a consequence

Uncertainty is embodied in much of the information gathered during the evaluation. There is uncertainty surrounding whether a threat will occur and whether the organization is sufficiently protected against the threat actor. Uncertainty is often represented using likelihood of occurrence, or probability.

In Activity S4.2, probability evaluation criteria were created for high, medium, and low threat probabilities.

Instructions

Step 24 (optional)

1. The table below highlights information for each active threat that you may have recorded on each critical asset's *Risk Profile Worksheet* (Vol. 5-8).

Type of Information	Step Number
Contextual information about threat actors	Step 13
The motive for deliberate actions by human actors	Step 14
The history of each active threat	Step 15
Areas of concern	Step 16

For each active threat, review any information you recorded for that threat.

Note: When you estimate probability, you will use a threat's history as a basis.

Consider the following question for each threat:

- How likely is the threat to occur in the future?

Review the history of the threat and assign that threat a qualitative probability value (high, medium, or low) based on the probability evaluation criteria that you created in Activity S4.2 (Step 23) and the history of that threat. Probability evaluation criteria are documented on the *Probability Evaluation Criteria Worksheet* (Vol. 4).

Note: Do **not** record probability values on the *Risk Profile Worksheet* (Vol. 5-8) at this time. You should not record probabilities until later in Step 24.

(continued on next page)

Activity S4.3: Evaluate Probabilities of Threats (cont.) Phase 3, Process S4, Step 24

Activity Worksheets	*Reference Worksheets*
• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	• Probability Evaluation Criteria (Vol. 4)

Instructions (cont.)

Step 24 (cont.)

2. Consider the following question for each threat:
   - Does any of the other information you recorded for the threat change the estimate based on history?

   Consider the following information you recoded on the *Risk Profile Worksheets* (Vol. 5-8):
   - motive for deliberate actions by human actors
   - summary of computing infrastructure vulnerabilities for network threats and malicious code (if it has been estimated)
   - summary of physical infrastructure vulnerabilities for physical threats (if it has been estimated)
   - contextual information about threat actors
   - specific examples of threats
3. Adjust your estimate of any threat probability if you believe that the information warrants it. Refer to the probability criteria when adjusting probability estimates.

   Document each probability on the *Risk Profile Worksheet* (Vol. 5-8) by recording
   - "H" for each high probability
   - "M" for each medium probability
   - "L" for each low probability

   Note: Because each branch on the threat tree represents multiple specific threats, you might identify multiple probabilities for a given threat; which could lead to more than one probability value for a given branch. If this happens, record the highest value for that impact area on the *Risk Profile Worksheet* (Vol. 5-8).

(continued on next page)

Activity S4.3: Evaluate Probabilities of Threats (cont.) Phase 3, Process S4, Step 24

Activity Worksheets	*Reference Worksheets*
• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	• Probability Evaluation Criteria (Vol. 4)

Instructions (cont.)

Step 24 (cont.)

4. Consider the following question for each threat:

   - How confident are you in your estimate of probability for this threat?

   Consider the following:

   - accuracy of history data
   - confidence in your estimate of motive strength (where applicable)
   - comprehensiveness of the evaluation of the computing infrastructure vulnerabilities (where applicable)
   - comprehensiveness of the evaluation of the physical infrastructure vulnerabilities (where applicable)

   Next to each threat probability value on the *Risk Profile Worksheet* (Vol. 5-8) is a scale for confidence with the following defined points: very much, somewhat, and not at all. Based on your answer to the above question, mark an 'X' on the scale at the point that indicates your confidence in the probability value for that threat. The following points are provided as references on the scale:

   - *Very* – You have a considerable amount of objective data related to your estimate. Any reasonable person reviewing the objective data would reach the same conclusion.
   - *Somewhat* – You have a limited amount of objective data related to your estimate. A reasonable person would need to make key inferences and assumptions to reach the same conclusion. However it is likely that a reasonable person would arrive at the same conclusion.
   - *Not at all* – You have little or no objective data related to your estimate. A reasonable person could arrive at a different conclusion because there are little or no objective data upon which to base the estimate.

(continued on next page)

Activity S4.3: Evaluate Probabilities of Threats (cont.) Phase 3, Process S4, Step 24

Activity Worksheets	*Reference Worksheets*
• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8)	• Probability Evaluation Criteria (Vol. 4)

Instructions (cont.)

Action Items, Notes, and Recommendations

1. Document all action items that you identified during Process S4 on the *Action List Worksheet* (Vol. 9).

   Remember to include the following information for each action item:

   - a description of the action
   - responsibility for completing the action
   - a date for completing the action
   - any management actions that could help facilitate completion of the action

2. Document notes relevant to the activities in Process S4 on the *Notes and Recommendations Worksheet* (Vol. 9).
3. Document all recommendations from Process S4 that you want to consider during Process S5 on the *Notes and Recommendations Worksheet* (Vol. 9).

Process S5: Develop Protection Strategy and Mitigation Plans

This process focuses on defining a protection strategy and mitigation plans as well as the next steps needed to implement the results of the OCTAVE-S evaluation.

S5.1 Describe Current Protection Strategy

Activity S5.1: Describe Current Protection Strategy	Phase 3, Process S5, Step 25
Activity Worksheets • Protection Strategy (Vol. 9)	*Reference Worksheets* • Security Practices (Vol. 4)

Background/Definitions

Protection Strategy – defines the overall strategy employed by an organization to enable, initiate, implement, and maintain its internal security. It is structured according to the security practice areas.

Characteristic – a quality or attribute of a security practice area. Each security practice area comprises multiple characteristics.

Approach – the way in which an organization addresses a characteristic of a security practice area

Task – an activity that must be completed as part of an operational security practice area

Security Practice Areas – groups of practices that are either strategic or operational. Strategic security practice areas are typically broad and tend to affect all risks to all critical assets equally (e.g., documenting a set of security policies for the organization). Operational security practice areas focus on day-to-day tasks and can be targeted toward mitigating specific risks to specific assets (e.g., checking a specific system for default accounts).

A protection strategy defines how an organization intends to raise or maintain the existing level of security. Its objective is to provide a direction for future information security efforts rather than to find an immediate solution to every security vulnerability and concern.

Since a protection strategy provides organizational direction with respect to information security activities, it is structured according to security practice areas. The security practice areas are illustrated in the table below.

Strategic Practice Areas	**Operational Practice Areas**
1. Security Awareness and Training	7. Physical Access Control
2. Security Strategy	8. Monitoring and Auditing Physical Security
3. Security Management	9. System and Network Management
4. Security Policies and Regulations	10. Monitoring and Auditing IT Security
5. Collaborative Security Management	11. Authentication and Authorization
6. Contingency Planning/Disaster Recovery	12. Vulnerability Management
	13. Encryption
	14. Security Architecture and Design
	15. Incident Management

(continued on next page)

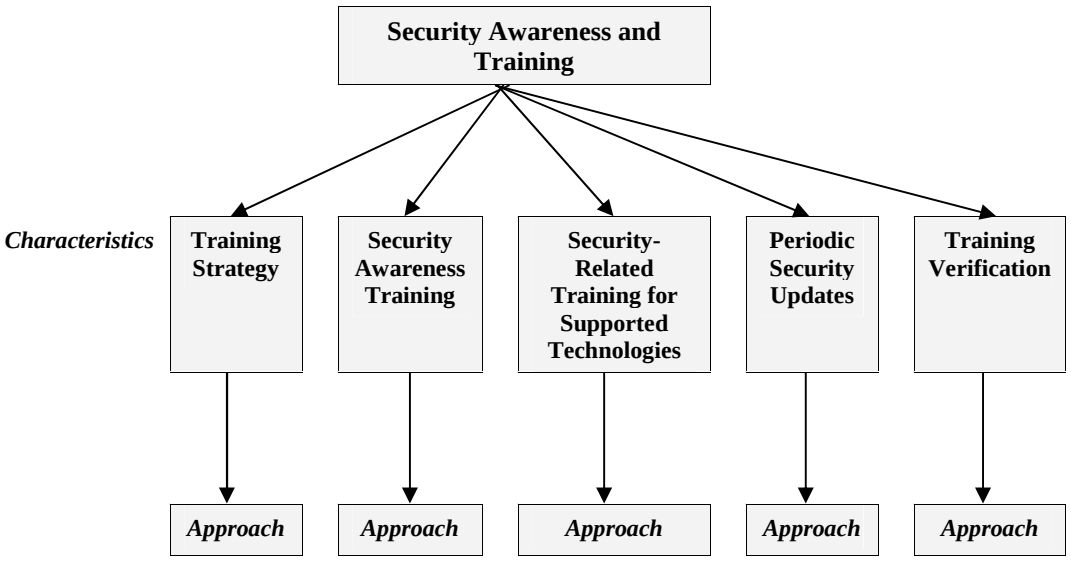
Activity S5.1: Describe Current Protection Strategy (cont.) Phase 3, Process S5, Step 25

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Background/Definitions (cont.)

In OCTAVE-S, each security practice area has multiple characteristics that must be addressed. The type of characteristics is different for strategic and operational security practice areas.

The following diagram depicts the characteristics for *Security Awareness and Training*, a strategic security practice area:



Each *strategic* security practice area has a unique set of characteristics. Refer to the *Protection Strategy Worksheet* (Vol. 9) to see the characteristics for the strategic security practice areas. The *Protection Strategy Worksheet* (Vol. 9) provides a range of approaches for each characteristic. Each characteristic will have a unique approach. For example, the range of approaches for *Training Verification* includes

- ❑ The organization has formal mechanisms for tracking and verifying that staff members receive appropriate security-related training.
- ❑ The organization has informal mechanisms for tracking and verifying that staff members receive appropriate security-related training.
- ❑ The organization has no mechanisms for tracking and verifying that staff members receive appropriate security-related training.
- ❑ _____

The blank is provided for any unique approaches implemented by an organization.

Note: Only one approach is selected for each characteristic of a strategic security practice area.

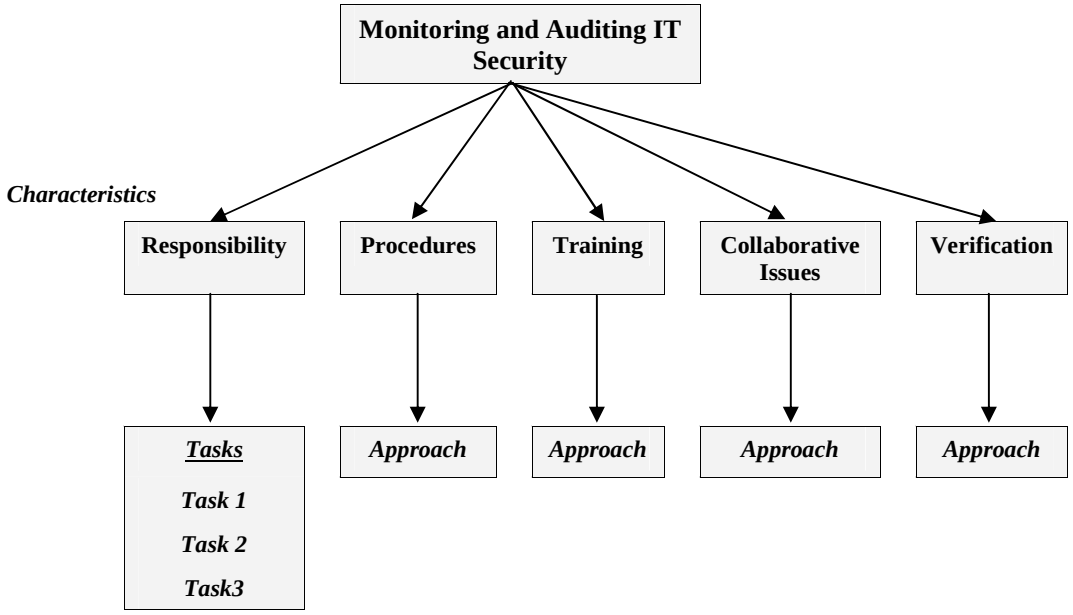
(continued on next page)

Activity S5.1: Describe Current Protection Strategy (cont.) Phase 3, Process S5, Step 25

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Background/Definitions (cont.)

The following diagram depicts the strategy for *Monitoring and Auditing IT Security*, an operational security practice area:



All *operational* security practice areas have identical characteristics (as illustrated above) with one exception. The *Encryption* security practice area breaks the *Training* characteristic into the following two characteristics: *Information Technology Training* and *Staff Training*. This is the only such exception for the operational security practice areas.

The *Responsibility* characteristic defines who has accountability for each task of an operational security practice area. Responsibility for a task can be assigned to people in your organization, to third parties, or to a combination of people in your organization and third parties.

If people from your organization have responsibility for some or all tasks of an operational security practice area, you need to assign an approach to the *Procedures* and *Training* characteristics.

If people from a third party have responsibility for some or all tasks of an operational security practice area, you need to assign an approach to the *Collaborative Issues* and *Verification* characteristics.

(continued on next page)

Activity S5.1: Describe Current Protection Strategy (cont.) Phase 3, Process S5, Step 25

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Background/Definitions (cont.)

Refer to the *Protection Strategy Worksheet* (Vol. 9) to see the characteristics for all operational security practice areas. The *Protection Strategy Worksheet* (Vol. 9) provides a range of tasks for the *Responsibility* characteristic and a range of approaches for the other characteristics.

For example, the range of tasks for the *Responsibility* characteristic of *Monitoring and Auditing IT Security* includes

- ❑ using system and network monitoring tools to track system and network activity
- ❑ auditing the firewall and other security components periodically for compliance with policy
- ❑ investigating and addressing any unusual activity that is identified
- ❑ _____

The blank is provided for any unique tasks required by an organization.

Note: You typically select multiple tasks for the *Responsibility* characteristic. However, for each of the remaining characteristics of an operational security practice area, only one approach is selected.

The range of approaches for the *Procedures* characteristic of *Monitoring and Auditing IT Security* includes

- ❑ The organization has formally documented procedures for monitoring network-based access to systems and networks.
- ❑ The organization has some formally documented procedures for monitoring network-based access to systems and networks. Some procedures in this area are informal and undocumented.
- ❑ The organization has informal and undocumented procedures for monitoring network-based access to systems and networks.
- ❑ _____

The blank is provided for any unique approaches implemented by an organization.

Note: The protection strategy and the security practices survey examine two different facets of security practice areas. The protection strategy describes the processes used to perform activities in each security practice area. The extent to which processes are formally defined is explored. The stoplight status on the security practices survey indicates how well the analysis team believes its organization is performing in each area. An organization could be performing very well in an area, but have very informal processes. Likewise, an organization could have significant room for improvement despite having very formal policies and procedures.

(continued on next page)

Activity S5.1: Describe Current Protection Strategy (cont.) Phase 3, Process S5, Step 25

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Instructions

Note: Before you begin Process S5, review any notes and recommendations you recorded on the *Notes and Recommendations Worksheet* (Vol. 9) during previous processes. These notes and recommendations could be relevant to the activities you will conduct during Process S5.

Also review all action items you recorded on the *Action List Worksheet* (Vol. 9) during previous processes. These action items could be relevant to the activities you will conduct during Process S5.

Step 25

Note: The characteristics for a strategic security practice area are different than those for an operational security practice area. The instructions examine how to address each type of security practice area separately.

1. Review the information contained on the *Security Practices Worksheet* (Vol. 4). Pay attention to the following information for each security practice area:
   - the stoplight status
   - the extent to which each security practice for an area is reflected in the organization
   - what the organization is currently doing well in an area
   - what the organization is not currently doing well in an area
2. Transfer the stoplight status for each security practice area (for both strategic *and* operational security practice areas) from the *Security Practices Worksheet* (Vol. 4) to the designated area on the *Protection Strategy Worksheet* (Vol. 9) before defining the strategy for that area.
3. Develop the protection strategy for each strategic security practice area. The following list includes all strategic security practice areas:

   Strategic Practice Areas

   1. Security Awareness and Training
   2. Security Strategy
   3. Security Management
   4. Security Policies and Regulations
   5. Collaborative Security Management
   6. Contingency Planning/Disaster Recovery

(continued on next page)

Activity S5.1: Describe Current Protection Strategy (cont.) Phase 3, Process S5, Step 25

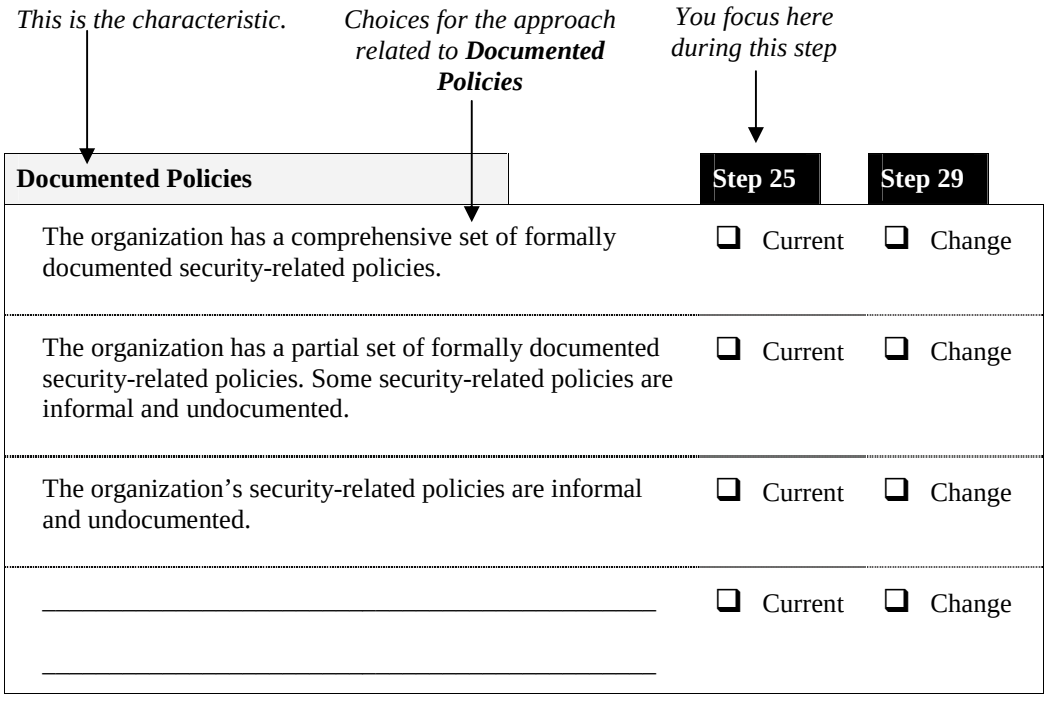
Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Instructions (cont.)

Step 25 (cont.)

4. Each strategic security practice area comprises several unique characteristics. For example, *Security Policies and Regulations* breaks down into the following characteristics:
   - Documented Policies
   - Policy Management
   - Policy Enforcement
   - Staff Awareness
   - Policy and Regulatory Compliance
   - Other

   The following diagram illustrates the *Documented Policies* characteristic for *Security Policies and Regulations*. Review the format of each strategic security practice area on the *Protection Strategy Worksheet* (Vol. 9).



(continued on next page)

Activity S5.1: Describe Current Protection Strategy (cont.) Phase 3, Process S5, Step 25

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Instructions (cont.)

Step 25 (cont.)

5. For each characteristic in a given strategic security practice area, consider the following question:

   - What is your organization's approach for addressing this characteristic?

   The *Protection Strategy Worksheet* (Vol. 9) provides several potential answers to the question for each characteristic. If one of the options matches the current situation in your organization, mark an 'X' in the box entitled "Current" next to that option.

   Make sure that you fill in any blanks provided for the option you select. You can change the words provided or add additional words as necessary.

   Note: You are provided with blank lines at the end of each characteristic. If you have a unique answer for how your organization addresses that characteristic, record the approach in the blanks provided and mark an 'X' in the box entitled "Current" next to the blanks.

   You are also provided a blank characteristic for each *strategic* security practice area. If you have a unique characteristic for an area, record your organization's approach in that characteristic and mark an 'X' in the box entitled "Current" next to the approach.

   Do **not** mark an 'X' in the box entitled "Change" at this time. You will consider changes to your organization's protection strategy in Step 32.

   Complete the *Protection Strategy Worksheet* (Vol. 9) for all strategic security practice areas. Make sure that you address all applicable characteristics for each strategic security practice area.

6. Develop the strategy for each operational security practice area. The following list includes all operational security practice areas:

   Operational Practice Areas

   7. Physical Access Control
   8. Monitoring and Auditing Physical Security
   9. System and Network Management
   10. Monitoring and Auditing IT Security
   11. Authentication and Authorization
   12. Vulnerability Management
   13. Encryption
   14. Security Architecture and Design
   15. Incident Management

(continued on next page)

Activity S5.1: Describe Current Protection Strategy (cont.) Phase 3, Process S5, Step 25

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Instructions (cont.)

Step 25 (cont.)

7. Each operational practice area comprises several characteristics. The format for all operational practice areas is fairly consistent. The following table describes each characteristic and when you need to address that characteristic.

Characteristic	Description
Responsibility	This characteristic defines who has responsibility for completing a set of specified tasks for an operational security practice area. The *Responsibility* characteristic includes multiple tasks for which accountability is assigned. This characteristic defines whether accountability for each task rests with people in your organization, with third parties, or with a combination of people in your organization as well as third parties.
Procedures	If people from your organization have responsibility for some or all tasks of an operational security practice area, you must address this characteristic. The *Procedures* characteristic defines the extent to which procedures for an operational security practice area are formally defined.
Training	If people from your organization have responsibility for some or all tasks of an operational security practice area, you must address this characteristic. The *Training* characteristic defines the approach for building staff members' skills in a practice area.
Collaborative Issues	If people from a third party have responsibility for some or all tasks of an operational security practice area, you must address this characteristic. The *Collaborative Issues* characteristic defines the degree to which requirements for an operational security practice area are formally communicated to each third party.
Verification	If people from a third party have responsibility for some or all tasks of an operational security practice area, you must address this characteristic. The *Verification* characteristic defines the degree to which each third party complies with the requirements for an operational security practice area.

Note: If **people in your organization** have sole responsibility for all tasks in an operational security practice area, do **not** complete a strategy for the *Collaborative Issues* and *Verification* characteristics. If **a third party** has sole responsibility for all tasks in an operational security practice area, do **not** complete a strategy for the *Procedures* and *Training* characteristics.

(continued on next page)

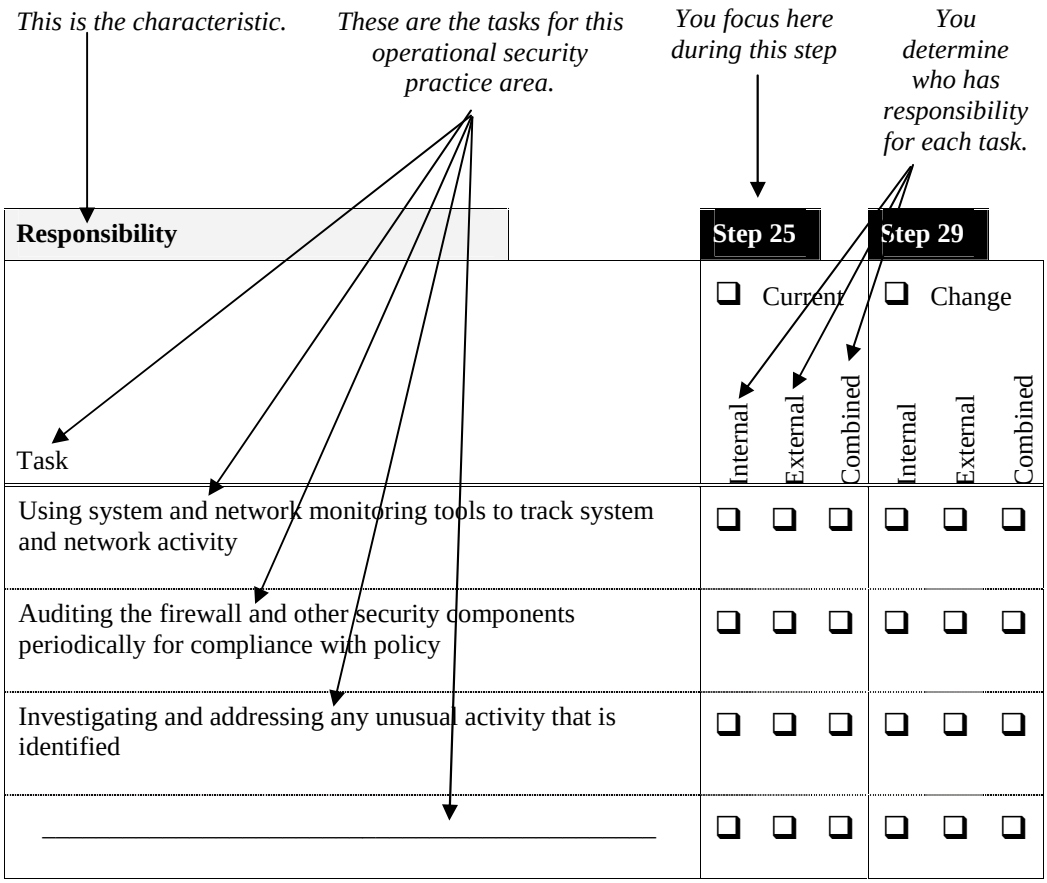
Activity S5.1: Describe Current Protection Strategy (cont.) Phase 3, Process S5, Step 25

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Instructions (cont.)

Step 25 (cont.)

The following diagram illustrates the *Responsibility* characteristic for *Monitoring and Auditing IT Security*.



Review the format of each operational security practice area on the *Protection Strategy Worksheet* (Vol. 9).

Note: The format of the *Responsibility* characteristic was highlighted here because it differs from the format of the other characteristics. The *Responsibility* characteristic for an operational security practice area comprises the tasks that must be performed in that practice area. Each of the other characteristics for an operational security practice area defines the approach for achieving that characteristic. The format of the other characteristics is similar to the format of the characteristics for the strategic security practice areas.

(continued on next page)

Activity S5.1: Describe Current Protection Strategy cont.) Phase 3, Process S5, Step 25

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Instructions (cont.)

Step 25 (cont.)

8. The *Protection Strategy Worksheet* (Vol. 9) lists several tasks under the *Responsibility* characteristic for each operational security practice area. Initially you determine who has responsibility for each task for an operational security practice area. First, mark an 'X' in the box entitled "Current."

   For each operational security practice area, consider the following questions:

   - Who is currently responsible for completing each task in this operational security practice area? People in your organization? A third party? A combination of people in your organization and one or more third parties?

   The *Protection Strategy Worksheet* (Vol. 9) lists three options under the current column for each task:

   - Internal – People in your organization are responsible for completing the task.
   - External – One or more third parties are responsible for completing the task.
   - Combined – A combination of people in your organization and one or more third parties are responsible for completing the task.

   Mark an 'X' in the appropriate box for each task. You can change the words provided for a task or add additional words as necessary.

   Note: The *Responsibility* characteristic for each operational security practice area provides several blanks. If you have tasks that are not listed in the protection strategy for an operational security practice area, record those tasks in the blanks provided and mark an 'X' in the appropriate box designating who is responsible for each task.

   Do **not** mark an 'X' in the box entitled "Change" at this time. You will consider changes to your organization's protection strategy in Step 29.

(continued on next page)

Activity S5.1: Describe Current Protection Strategy (cont.) Phase 3, Process S5, Step 25

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Instructions (cont.)

Step 25 (cont.)

9. If people from your organization have responsibility for some or all tasks of an operational security practice area, you must designate an approach for the *Procedures* and *Training* characteristics

   Note: The *Encryption* security practice area breaks training into *Information Technology Training* and *Staff Training*. This is the only such exception in the operational security practice areas.

   For the *Procedures* and *Training* characteristics in a given operational security practice area, consider the following question:

   - What is your organization's approach for addressing this characteristic?

   The *Protection Strategy Worksheet* (Vol. 9) provides several potential answers to the question for each characteristic. If one of the options matches the current situation in your organization, mark an 'X' in the box entitled "Current" next to that option.

   Make sure that you fill in any blanks provided for the option you select. You can change the words provided or add additional words as necessary.

   Note: You are provided with blank lines at the end the *Procedures* and *Training* characteristics. If you have a unique approach for how your organization addresses one of those characteristics, record that approach in the blanks provided and mark an 'X' in the box entitled "Current" next to the blanks.

   Do **not** mark an 'X' in the box entitled "Change" at this time. You will consider changes to your organization's protection strategy in Step 29.

(continued on next page)

Activity S5.1: Describe Current Protection Strategy (cont.) Phase 3, Process S5, Step 25

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Security Practices (Vol. 4)

Instructions (cont.)

Step 25 (cont.)

10. If people from a third party have responsibility for some or all tasks of an operational security practice area, you must designate an approach for the *Collaborative Issues* and *Verification* characteristics. Record the name of the third party in the space provided.

    Note: You might have more than one third party providing information security services in an operational security practice area. Complete *Collaborative Issues* and *Verification* characteristics for each third party that provides services in that area.

    For each such characteristic in a given operational security practice area, consider the following question:

    - What is your organization's approach for addressing this characteristic?

    The *Protection Strategy Worksheet* (Vol. 9) provides several potential answers to the question for each characteristic. If one of the options matches the current situation in your organization, mark an 'X' in the box entitled "Current" next to that option.

    Make sure that you fill in any blanks provided for the option you select. You can change the words provided or add additional words as necessary.

    Note: You are provided with blank lines at the end the *Collaborative Issues* and *Verification* characteristics. If you have a unique answer for how your organization addresses one of those characteristics, record the approach in the blanks provided and mark an 'X' in the box entitled "Current" next to the blanks.

    Do **not** mark an 'X' in the box entitled "Change" at this time. You will consider changes to your organization's protection strategy in Step 29.

11. Complete the *Protection Strategy Worksheet* (Vol. 9) for all operational security practice areas. Make sure that you address all applicable characteristics for each operational security practice area.

S5.2 Select Mitigation Approaches

Activity S5.2: Select Mitigation Approaches	Phase 3, Process S5, Steps 26-27
Activity Worksheets • Risk Profile (Vol. 5-8)	*Reference Worksheets* • Impact Evaluation Criteria (Vol. 4) • Probability Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Infrastructure Review (Vol. 4) • Notes and Recommendations (Vol. 9)

Background/Definitions

Mitigation approach – how an organization intends to address a risk. An organization has the following options for each risk: accept, mitigate, or defer.

Accept – a decision made during risk analysis to take no action to address a risk and to accept the consequences should the risk occur. Risks that are accepted typically have a low impact on an organization.

Mitigate – a decision made during risk analysis to address a risk by implementing activities designed to counter the underlying threat. Risks that are mitigated typically have a high impact on an organization.

Defer – a situation where a risk is neither accepted nor mitigated. The impact on the organization due to a deferred risk is above a minimal threshold, but not so large as to be an immediate priority. Deferred risks are watched and reevaluated at some point in the future.

Mitigation area – a security practice area that is designated to be improved in order to mitigate one or more of an organization's security risks

The decision to accept a risk, mitigate it, or defer the decision is based on a number of factors. Impact value is often the primary driver when making the decision. Probability may be used to determine which risks to mitigate first.

Unfortunately, there is no lockstep decision-making process that applies in all circumstances. The risk profile created for each critical asset during OCTAVE-S is a decision support tool. It presents threats, impact values for multiple impact areas, probability values, and the stoplight statuses of the security practice areas, illustrating a picture of the risks affecting that critical asset. An analysis team uses the risk profile to support the mitigation decisions that it makes.

(continued on next page)

Activity S5.2: Select Mitigation Approaches (cont.)	Phase 3, Process S5, Steps 26-27
Activity Worksheets • Risk Profile (Vol. 5-8)	*Reference Worksheets* • Impact Evaluation Criteria (Vol. 4) • Probability Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Infrastructure Review (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions

Step 26

Transfer the stoplight status for each security practice area from the *Security Practices Worksheet* (Vol. 9) to the "Security Practice Areas" section (Step 29) of each critical asset's *Risk Profile Worksheet* (Vol. 5-8).

Note: Some of the security practice areas are "blocked" for each risk. These areas are unlikely to be selected as mitigation areas. Do not record the stoplight status for an area that is "blocked," unless you have determined that it applies to a risk under your current circumstances.

Step 27

Note: There is no single approach for analyzing the information that you recorded throughout the evaluation. One approach is documented in these guidelines. You can select your approach to best suit your analysis team's preferences as well as your organization's accepted practices.

Your ultimate goal in Step 27 is to select three security practice areas as mitigation areas. Based on your organization's security risks as well as funding and staff constraints, you might decide to select fewer or more than three mitigation areas. Use your best judgment.

1. Review the information contained on the following worksheets:
    - *Risk Profile Worksheet* (for each critical asset) (Vol. 5-8)
    - *Critical Asset Worksheet* (for each critical asset) (Vol. 5-8)
    - *Security Practices Worksheet* (Vol. 4)
    - *Infrastructure Review Worksheet* (Vol. 4)

    You might need additional context for interpreting the impact, probability, and vulnerability data on the above worksheets. Review your definitions of impact and probability severity levels on the following worksheets:
    - *Impact Evaluation Criteria Worksheet* (Vol. 4)
    - *Probability Evaluation Criteria Worksheet* (Vol. 4)

(continued on next page)

Activity S5.2: Select Mitigation Approaches (cont.) Phase 3, Process S5, Steps 26-27

Activity Worksheets	*Reference Worksheets*
• Risk Profile (Vol. 5-8)	• Impact Evaluation Criteria (Vol. 4) • Probability Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Infrastructure Review (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions (cont.)

Step 27 (cont.)

2. Review all information you recorded throughout the evaluation on the *Notes and Recommendation Worksheets* (Vol. 9). Pay specific attention to any recommendations that you made regarding potential mitigation activities.

   Note: You can review any information that you recorded during the evaluation before you select mitigation approaches. The worksheets highlighted above constitute the minimal set of information you will need during this activity.

3. Consider the following questions:

   - What is driving your selection of mitigation areas?
   - Which impact areas are most important to your organization?
   - How will you factor probability into your decisions?
   - Which security requirement is most important for each critical asset?
   - Which specific areas of concern do you need to address?
   - Which specific security practice areas need the most improvement?
   - Which specific organizational vulnerabilities do you need to address?
   - What other factors will influence your selection of mitigation areas?

   Review risks to your critical assets, keeping the above questions in mind. Start thinking about how to address each risk. You need to start thinking about which risks you intend to mitigate, which you intend to accept, and which you intend to watch and reevaluate at some point in the future.

4. Consider the following question:

   - Which risks need to be mitigated?

   Mark an 'X' in the box entitled "Mitigate" for each risk that you intend to mitigate. Think ahead as you are selecting which risks to mitigate. If you select too many areas, you could be overwhelmed during mitigation planning.

(continued on next page)

Activity S5.2: Select Mitigation Approaches (cont.) Phase 3, Process S5, Steps 26-27

Activity Worksheets	*Reference Worksheets*
• Risk Profile (Vol. 5-8)	• Impact Evaluation Criteria (Vol. 4) • Probability Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Infrastructure Review (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions (cont.)

Step 27 (cont.)

5. Consider the following question for all risks that have not yet been assigned a mitigation approach:

   - Which risks are you going to accept?

   Think about the impact on the organization due to each risk. Determine which impacts are low enough that you do not foresee the need to ever take proactive action to prevent them.

   Mark an 'X' in the box entitled "Accept" for these risks in the designated area (Step 27) on the *Risk Profile Worksheet* (Vol. 5-8).

6. For any risks that have still not been assigned a mitigation approach (i.e., those not yet designated as "Mitigate" or "Accept"), consider the following question:

   - Are there any additional risks that you need to mitigate?

   Remember to consider your decision-making drivers as you consider additional areas to select. Mark an 'X' in the box entitled "Mitigate" for each additional risk that you select.

7. To this point, you have selected risks that the organization will mitigate and also identified those risks that the organization will accept. You also likely have some risks that have neither been accepted nor mitigated.

   For those risks that have neither been accepted nor mitigated, you have decided that the potential impacts resulting from these risks were not low enough to accept nor large enough to be designated as a current mitigation priority. Mark an 'X' in the box entitled "Defer" for these risks. Deferred risks are watched and reevaluated at some point in the future.

   You have now assigned a mitigation approach to each risk. Next, you need to select mitigation areas.

(continued on next page)

Activity S5.2: Select Mitigation Approaches (cont.)	Phase 3, Process S5, Steps 26-27
Activity Worksheets • Risk Profile (Vol. 5-8)	*Reference Worksheets* • Impact Evaluation Criteria (Vol. 4) • Probability Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Infrastructure Review (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions (cont.)

Step 27 (cont.)

8. Consider the following questions as you review the risks to all critical assets, also keeping in mind your decision-making drivers:
    - Which security practice areas have the most room for improvement? How would these areas affect the risks that need to be mitigated?
    - Which security practice areas, if selected for mitigation, could mitigate many risks to more than one critical asset?
    - Are there any regulations or policies that need to be considered as you select mitigation areas? If so, which areas would they lead you to select?

    Select three (3) security practice areas as mitigation areas. Be sure to consider any constraints (e.g., funds and staff) when you make your selections. If your situation warrants it, you can select fewer or more than three security practice areas. You must use your best judgment when deciding how many areas to select.

    Note: Once you decide to implement improvements in a security practice area to mitigate your organization's security risks, those practice areas are referred to as mitigation areas.

    For each risk that you have decided to mitigate, circle on the appropriate *Risk Profile Worksheet* (Vol. 5-8) which of the selected security practice areas will mitigate that risk.

(continued on next page)

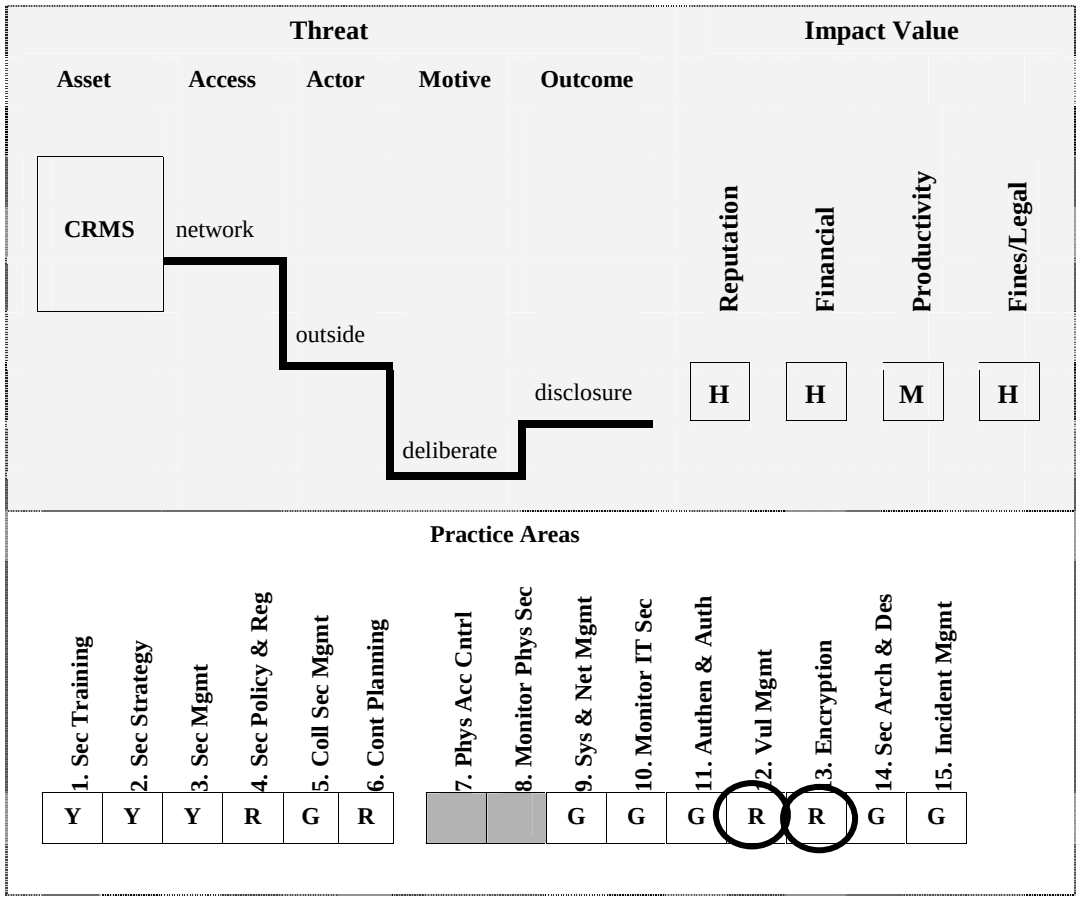
Activity S5.2: Select Mitigation Approaches (cont.) Phase 3, Process S5, Steps 26-27

Activity Worksheets	*Reference Worksheets*
• Risk Profile (Vol. 5-8)	• Impact Evaluation Criteria (Vol. 4) • Probability Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Infrastructure Review (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions (cont.)

Step 27 (cont.)

The following example illustrates how two mitigation areas (*Vulnerability Management* and *Encryption*) are circled on the *Risk Profile Worksheet* for one risk being mitigated:



(continued on next page)

Activity S5.2: Select Mitigation Approaches (cont.)	Phase 3, Process S5, Steps 26-27
Activity Worksheets • Risk Profile (Vol. 5-8)	*Reference Worksheets* • Impact Evaluation Criteria (Vol. 4) • Probability Evaluation Criteria (Vol. 4) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Infrastructure Review (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions (cont.)

Step 27 (cont.)

When you select security practice areas to mitigate your organization's security risks, it is recommended that you also record those areas as well as your rationale for selecting them on the *Notes and Recommendations Worksheet* (Vol. 9).

Remember, there is no single approach for analyzing the information that you recorded throughout the evaluation. Assigning mitigation approaches is not a lockstep process. Different teams will approach the analysis in different ways. Most analysis approaches require considerable discussion and some iteration.

These guidelines present one approach for selecting mitigation approaches and mitigation areas. You can tailor the approach to best suit your analysis team's preferences as well as your organization's accepted practices

S5.3 Develop Risk Mitigation Plans

Activity S5.3: Develop Risk Mitigation Plans	Phase 3, Process S5, Step 28
Activity Worksheets • Mitigation Plan (Vol. 9)	*Reference Worksheets* • Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Protection Strategy (Vol. 9) • Action List (Vol. 9) • Notes and Recommendations (Vol. 9) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

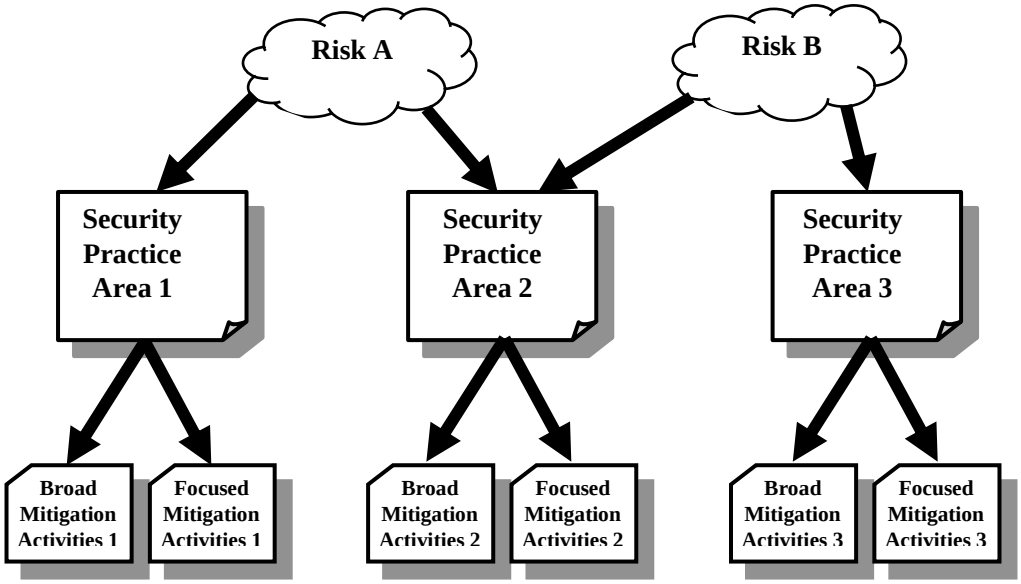
Background/Definitions

Risk mitigation plan – a plan that is intended to reduce the risks to a critical asset. Risk mitigation plans tend to incorporate activities, or countermeasures, designed to counter the threats to the assets.

An analysis team creates a separate mitigation plan for each security practice area it selected as a mitigation area during the previous activity (Activity S5.2).

There are two types of mitigation activities: broad mitigation activities and focused mitigation activities.

The following diagram illustrates the relationships among risks, security practice areas, and mitigation activities.



(continued on next page)

Activity S5.3: Develop Risk Mitigation Plans (cont.) Phase 3, Process S5, Step 28

Activity Worksheets	*Reference Worksheets*
• Mitigation Plan (Vol. 9)	• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Protection Strategy (Vol. 9) • Action List (Vol. 9) • Notes and Recommendations (Vol. 9) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Background/Definitions (cont.)

Broad mitigation activities trigger a change in the approach for a security practice area's characteristic. Focused mitigation activities

- do not require a change to the approach for a security practice area's characteristic
- improve how the current approach for a security practice area's characteristic is implemented

Focused mitigation activities are often directed at specific assets or concentrated on specific improvements.

Risk mitigation plans are often linked to enterprise survivability. They are generally designed to reduce the risks that could prevent an organization from achieving its mission by addressing the underlying threats. A mitigation activity can address threats in one or more of the following ways:

- *Recognize* threats as they occur.
- *Resist* threats to prevent them from occurring.
- *Recover* from threats after they occur.

Risk mitigation plans comprise the following elements:

- *mitigation activity* – defines the activities an analysis team is recommending to implement in a security practice area
- *rationale* – documents the reasons for selecting each mitigation activity. The rationale should document whether the activity is intended to recognize threats, resist them, or recover from them.
- *mitigation responsibility* – identifies who must be involved in implementing each activity
- *additional support* – documents any additional support that will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)

(continued on next page)

Activity S5.3: Develop Risk Mitigation Plans (cont.) Phase 3, Process S5, Step 28

Activity Worksheets	*Reference Worksheets*
• Mitigation Plan (Vol. 9)	• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Protection Strategy (Vol. 9) • Action List (Vol. 9) • Notes and Recommendations (Vol. 9) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions

Step 28

1. Review the information contained on the following worksheets:
   - *Risk Profile Worksheet* (for each critical asset) (Vol. 5-8)
   - *Security Practices Worksheet* (Vol. 4)
   - *Protection Strategy Worksheet* (Vol. 9)
   - *Action List Worksheet* (Vol. 9)
   - *Critical Asset Information Worksheet* (for each critical asset) (Vol. 5-8)

   You might need additional context for interpreting the impact, probability, and vulnerability data on the above worksheets. Review your definitions of impact, probability, and vulnerability severity levels on the following worksheets:
   - *Impact Evaluation Criteria Worksheet* (Vol. 4)
   - *Probability Evaluation Criteria Worksheet* (Vol. 4)
2. Review all information that you recorded throughout the evaluation on the *Notes and Recommendation Worksheets* (Vol. 9). Pay specific attention to any recommendations that you made regarding potential mitigation activities.

   Note: You can review any information that you recorded during the evaluation before you select mitigation approaches. The worksheets highlighted above constitute the minimal set of information you will need during this activity.
3. In this step, you create mitigation plans for each security practice area that you selected during the previous activity. For each area you selected, review the range of candidate mitigation activities in the *Candidate Mitigation Activities Guide* for that area. The guide provides possible mitigation activities, but not an exhaustive list. Do not be limited by the activities listed in the guide.

(continued on next page)

Activity S5.3: Develop Risk Mitigation Plans (cont.) Phase 3, Process S5, Step 28

Activity Worksheets	*Reference Worksheets*
• Mitigation Plan (Vol. 9)	• Risk Profile in appropriate Critical Asset Workbook (Vol. 5-8) • Security Practices (Vol. 4) • Protection Strategy (Vol. 9) • Action List (Vol. 9) • Notes and Recommendations (Vol. 9) • Critical Asset Information in appropriate Critical Asset Workbook (Vol. 5-8)

Instructions (cont.)

Step 28 (cont.)

4. Consider the following question for each selected mitigation area:
    - What mitigation activities would reduce the risk(s) that led to the selection of this area?
    - What is the rationale for selecting each activity?
    - Who needs to be involved in implementing each activity? Why?
    - What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?

    Develop a mitigation plan for each area you selected.

    Note: Look for instances where you anticipate that an activity will trigger a change to the protection strategy (i.e., broad mitigation activities). Make sure that you record this information in the "Mitigation Activity" area for that activity.

S5.4 Identify Changes to Protection Strategy

Activity S5.4: Identify Changes to Protection Strategy	Phase 3, Process S5, Step 29
Activity Worksheets • Protection Strategy (Vol. 9)	*Reference Worksheets* • Mitigation Plan (Vol. 9) • Security Practices (Vol. 4) • Notes and Recommendations (Vol. 9)

Background/Definitions

An organization's protection strategy defines the approaches used by an organization to enable, initiate, implement, and maintain its internal security, providing a direction for future information security efforts. The protection strategy is structured according to security practice areas highlighted in the table below.

Strategic Practice Areas	**Operational Practice Areas**
1. Security Awareness and Training	7. Physical Access Control
2. Security Strategy	8. Monitoring and Auditing Physical Security
3. Security Management	9. System and Network Management
4. Security Policies and Regulations	10. Monitoring and Auditing IT Security
5. Collaborative Security Management	11. Authentication and Authorization
6. Contingency Planning/Disaster Recovery	12. Vulnerability Management
	13. Encryption
	14. Security Architecture and Design
	15. Incident Management

During Activity S5.1 of OCTAVE-S, an analysis team defines its organization's current protection strategy. During Activity S5.2, the team selects which security practice areas must be improved to mitigate the organization's highest priority risks. Then, during Activity S5.3, the team develops mitigation plans for each security practice area selected as a mitigation area.

Risk mitigation plans can include two types of activities: broad mitigation activities and focused mitigation activities. Broad mitigation activities typically trigger a change in the organization's protection strategy, while focused activities improve how the current protection strategy is implemented. *Each change to the protection strategy must be documented*. Documenting changes to an organization's protection strategy is the goal of Activity S5.4.

(continued on next page)

Activity S5.4: Identify Changes to Protection Strategy (cont.) Phase 3, Process S5, Step 29

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Mitigation Plan (Vol. 9) • Security Practices (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions

Step 29

1. Review the information contained on the following worksheets:
   - *Mitigation Plan Worksheet* (Review each plan.) (Vol. 9)
   - *Protection Strategy Worksheet* (Review the current strategy.) (Vol. 9)
   - *Security Practices Worksheet* (Vol. 4)
   - *Notes and Recommendations Worksheet* (Vol. 9)

   Note: You can review any information that you recorded during the evaluation before you perform this activity. The worksheets highlighted above constitute the minimal set of information you will need during this activity.

2. The diagrams on the next two pages illustrate the areas of the *Protection Strategy Worksheet* (Vol. 9) on which you will focus during this activity.

   Each security practice area comprises several characteristics. The following diagram illustrates the *Documented Policies* characteristic for *Security Policies and Regulations*. This characteristic is typical of most characteristics on the *Protection Strategy Worksheet* (Vol. 9). The exception is the *Responsibility* characteristic (for operational security practice areas), which is shown after the diagram for *Documented Policies*.

(continued on next page)

Activity S5.4: Identify Changes to Protection Strategy (cont.) Phase 3, Process S5, Step 29

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Mitigation Plan (Vol. 9) • Security Practices (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions (cont.)

Step 29 (cont.)

This is the characteristic.

*Choices for the approach related to **Documented Policies***

You focus here during this step

Documented Policies	**Step 25**	**Step 29**
The organization has a comprehensive set of formally documented security-related policies.	❑ Current	❑ Change
The organization has a partial set of formally documented security-related policies. Some security-related policies are informal and undocumented.	❑ Current	❑ Change
The organization's security-related policies are informal and undocumented.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

(continued on next page)

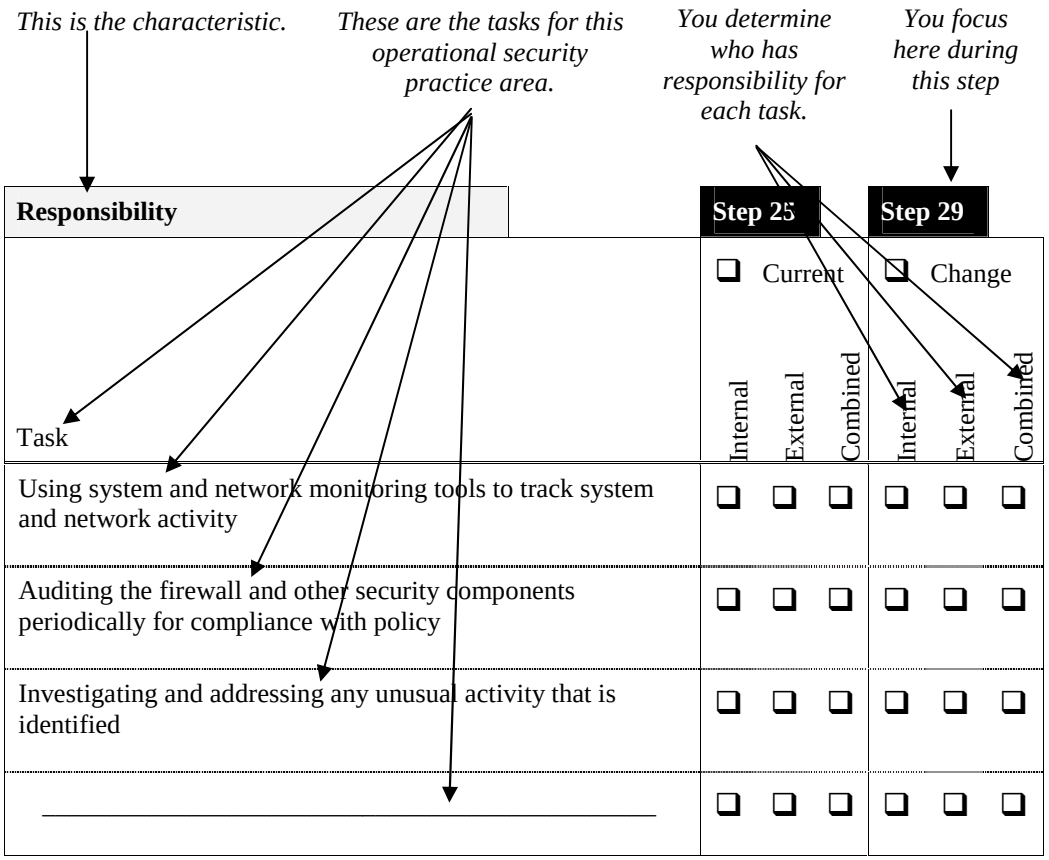
Activity S5.4: Identify Changes to Protection Strategy (cont.) Phase 3, Process S5, Step 29

Activity Worksheets	*Reference Worksheets*
• Protection Strategy (Vol. 9)	• Mitigation Plan (Vol. 9) • Security Practices (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions (cont.)

Step 29 (cont.)

The following diagram illustrates the *Responsibility* characteristic for *Monitoring and Auditing IT Security*.



Review the format of the protection strategy for each security practice area.

(continued on next page)

Activity S5.4: Identify Changes to Protection Strategy (cont.)	Phase 3, Process S5, Step 29
Activity Worksheets • Protection Strategy (Vol. 9)	*Reference Worksheets* • Mitigation Plan (Vol. 9) • Security Practices (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions (cont.)

Step 29 (cont.)

3. Consider the following questions for each mitigation activity that you identified during Activity S5.3:
    - Does this mitigation activity indicate a change in the organization's protection strategy?
    - Which characteristic in the security practice area would be affected? How would it be affected?

    If you determine that a mitigation activity affects one of the characteristics in a security practice area, mark an 'X' in the box entitled "Change" next the new approach on the *Protection Strategy Worksheet* (Vol. 9).

    Make sure that you fill in any blanks provided for the option you select. You can change the words provided or add additional words as necessary.

    Note: You are provided with blank lines at the end the all characteristics. If you have a unique answer for your organization's approach for a characteristic, record that strategy in the blanks provided and mark an 'X' in the box entitled "Change" next to the blanks.

4. Review the *Protection Strategy Worksheet* (Vol. 9). Examine the current strategy as well as any changes to the strategy you have identified. Consider the following question as you review the protection strategy:
    - Do you want to make any additional changes to the protection strategy?

    If your answer is yes, then mark those changes on the *Protection Strategy Worksheet* (Vol. 9).

    Next, you need to decide which risks, if any, are driving this change in the protection strategy. Return to the *Risk Profile Worksheet* (Vol. 5-8). Note which risks drove the selection of the new strategy by circling the corresponding security practice area on the appropriate *Risk Profile Worksheet*(s) (Vol. 5-8). (That is, complete Step 26.)

    It is possible that a change in the protection strategy is being driven by factors other than risk (e.g., policy, regulation). If this is the case, you do not need to circle any security practice areas on the *Risk Profile Worksheets* (Vol. 5-8).

    In either case, identify one or more activities that will produce the protection strategy change you identified and document them in the mitigation plan for the appropriate security practice area.

    Note: For any change to the protection strategy that is driven by factors other than risk, be sure to document those factors in the "Rationale" area for that activity.

(continued on next page)

Activity S5.4: Identify Changes to Protection Strategy (cont.)	Phase 3, Process S5, Step 29
Activity Worksheets • Protection Strategy (Vol. 9)	*Reference Worksheets* • Mitigation Plan (Vol. 9) • Security Practices (Vol. 4) • Notes and Recommendations (Vol. 9)

Instructions (cont.)

Action Items

Make sure that you document all action items that you identified during Process S6 on the *Action List Worksheet* (Vol. 9).

Remember to include the following information for each action item:

- a description of the action
- responsibility for completing the action
- a date for completing the action
- any management actions that could help facilitate completion of the action

S5.5 Identify Next Steps

Activity S5.5: Identify Next Steps	Phase 3, Process S5, Step 30
Activity Worksheets • Next Steps (Vol. 9)	*Reference Worksheets* • Protection Strategy (Vol. 9) • Mitigation Plan (Vol. 9) • Action List (Vol. 9)

Background/Definitions

Creating a set of next steps marks the end of OCTAVE-S. This activity requires the analysis team to consider what must be done to facilitate implementation of the evaluation's results. Next steps typically address the following four areas:

- management sponsorship for security improvement – defining what management must do to support the implementation of OCTAVE-S results
- monitoring implementation – identifying what the organization will do to track progress and ensure that the results of OCTAVE-S are implemented
- expanding the current information security risk evaluation – determining whether the organization needs to expand the current OCTAVE-S evaluation to include additional critical assets or additional operational areas
- next information security risk evaluation – determining when the organization will conduct its next OCTAVE-S evaluation

Instructions

Step 30

1. Review (at a minimum) the information contained on the following worksheets:
   - *Mitigation Plan Worksheet*s (Vol. 9)
   - *Protection Strategy Worksheet* (Vol. 9)
   - *Action List Worksheet* (Vol. 9)

   Consider the following questions:
   - What must management do to support the implementation of OCTAVE-S results?
   - What will the organization do to track progress and ensure that the results of this evaluation are implemented?
   - Will you expand the current OCTAVE-S evaluation to include additional critical assets? Which ones?
   - When will the organization conduct its next OCTAVE-S evaluation?

   Note: The above questions focus on what the senior managers plan to do to enable and encourage implementation of the evaluation results as well as ongoing security improvement activities.

   Determine what steps your organization must take to implement the results of this evaluation. Record those steps on the *Next Steps Worksheet* (Vol. 9).

(continued on next page)

Activity S5.5: Identify Next Steps (cont.) Phase 3, Process S5, Step 30

Activity Worksheets	*Reference Worksheets*
• Next Steps (Vol. 9)	• Protection Strategy (Vol. 9) • Mitigation Plan (Vol. 9) • Action List (Vol. 9)

Instructions

Step 30 (cont.)

2. At this point, you have completed an OCTAVE-S evaluation. Make sure that you formally document the results of this evaluation. The format for documenting OCTAVE-S results should fit your organization's normal documentation guidelines and should be tailored to meet your organization's needs.

   Note: It is important to establish a permanent record of evaluation results. The information that you record can serve as source material for subsequent evaluations and is also useful when tracking the status of plans and actions after the evaluation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
OCTAVE-S Implementation Guide, Version 1.0, Volume 3	F19628-00-C-0003

6. AUTHOR(S)

Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody

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

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

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

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

14. SUBJECT TERMS	15. NUMBER OF PAGES
information security, risk management, OCTAVE	94

16. PRICE CODE

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

OCTAVE®-S Implementation Guide, Version 1.0

Volume 4: Organizational Worksheets

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

HANDBOOK
CMU/SEI-2003-HB-003

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

OCTAVE®-S Implementation Guide, Version 1.0

Volume 4: Organizational Worksheets

CMU/SEI-2003-HB-003

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

Networked Systems Survivability Program

This report was prepared for the

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

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

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

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

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

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

Table of Contents

List of Tables

About This Document

This document is Volume 4 of the *OCTAVE-S Implementation Guide*, a 10-volume handbook supporting the OCTAVE-S methodology. This volume provides the worksheets that are completed once for the organization during an evaluation. These worksheets reflect information that is independent of any specific asset.

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℠ (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 Introduction

This document contains the Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE®)-S worksheets that are completed once during an evaluation. The activities that require these worksheets are asset-independent, indicating an organizational focus and relevance across all critical assets.

Table 1 provides a brief introduction to the contents of this workbook, using activity step numbers as a key. For more details about how to complete each step, refer to the *OCTAVE®-S Method Guidelines*, which can be found in Volume 3 of the *OCTAVE®-S Implementation Guide*.

Table 1: Worksheets Provided in This Workbook

Step	Description	Worksheet	Activity	Pages
Step 1	Define a qualitative set of measures (high, medium, low) against which you will evaluate a risk's effect on your organization's mission and business objectives.	Impact Evaluation Criteria	Phase 1 Process S1 S1.1 Establish Impact Evaluation Criteria	5-18
Step 2	Identify information-related assets in your organization (information, systems, applications, people).	Asset Identification	Phase 1 Process S1 S1.2 Identify Organizational Assets	19-28
Step 3a	Determine to what extent each practice in the survey is used by the organization.	Security Practices	Phase 1 Process S1 S1.3 Evaluate Organizational Security Practices	29-60

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

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

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 3b	As you evaluate each security practice area using the survey from Step 3a, document detailed examples of • what your organization is currently doing well in this area (security practices) • what your organization is currently *not* doing well in this area (organizational vulnerabilities)	Security Practices	Phase 1 Process S1 S1.3 Evaluate Organizational Security Practices	29-60
Step 4	After completing Steps 3a and 3b, assign a stoplight status (red, green, yellow) to each security practice area. The stoplight status should reflect how well you believe your organization is performing in each area.	Security Practices	Phase 1 Process S1 S1.3 Evaluate Organizational Security Practices	29-60
Step 5	Review the information-related assets that you identified during Step 2 and select up to five assets that are most critical to the organization.	Critical Asset Selection	Phase 1 Process S2 S2.1 Select Critical Assets	61-64
Step 19a	Document the classes of components that are related to one or more critical assets and that can provide access to those assets. Mark the path to each class selected in Steps 18a-18e. Note any relevant subclasses or specific examples when appropriate.	Infrastructure Review	Phase 2 Process S3 S4.2 Analyze Technology-Related Processes	65-70
Step 19b	For each class of components documented in Step 19a, note which critical assets are related to that class.	Infrastructure Review	Phase 2 Process S3 S4.2 Analyze Technology-Related Processes	65-70
Step 20	For each class of components documented in Step 19a, note the person or group responsible for maintaining and securing that class of component.	Infrastructure Review	Phase 2 Process S3 S4.2 Analyze Technology-Related Processes	65-70

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 21	For each class of components documented in Step 19a, note the extent to which security is considered when configuring and maintaining that class. Also record how you came to that conclusion. Finally, document any additional context relevant to your infrastructure review.	Infrastructure Review	Phase 2 Process S3 S4.2 Analyze Technology-Related Processes	65-70
Step 23	Define a qualitative set of measures (high, medium, low) against which you will evaluate the likelihood of a threat occurring.	Probability Evaluation Criteria	Phase 3 Process S4 S4.2 Establish Probability Evaluation Criteria	71-73

2 Impact Evaluation Criteria Worksheet

	Phase 1 Process S1 Activity S1.1
Step 1	Define a qualitative set of measures (high, medium, low) against which you will evaluate a risk's effect on your organization's mission and business objectives.

Step 1

Reputation/Customer Confidence

Impact Type	Low Impact
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.
Customer Loss	Less than _____% reduction in customers due to loss of confidence
Other:	
Other:	

Reputation/Customer Confidence	
Medium Impact	**High Impact**
Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
_____to _____% reduction in customers due to loss of confidence	More than _____% reduction in customers due to loss of confidence

Step 1

Financial

Impact Type	Low Impact
Operating Costs	Increase of less than _____% in yearly operating costs
Revenue Loss	Less than _____% yearly revenue loss
One-Time Financial Loss	One-time financial cost of less than $_____
Other:	

Financial	
Medium Impact	**High Impact**
Yearly operating costs increase by _____to _____%.	Yearly operating costs increase by more than _____%.
_____to _____% yearly revenue loss	Greater than _____% yearly revenue loss
One-time financial cost of $_____ to $_____	One-time financial cost greater than $_____

Step 1

Productivity

Impact Type	Low Impact
Staff Hours	Staff work hours are increased by less than _____% for _____to _____ day(s).
Other:	
Other:	
Other:	

Productivity	
Medium Impact	**High Impact**
Staff work hours are increased between _____% and _____% for _____to _____ day(s).	Staff work hours are increased by greater than _____% for _____to _____ day(s).

Step 1

Safety/Health

Impact Type	Low Impact
Life	No loss or significant threat to customers' or staff members' lives
Health	Minimal, immediately treatable degradation in customers' or staff members' health with recovery within four days
Safety	Safety questioned
Other:	

Safety/Health	
Medium Impact	**High Impact**
Customers' or staff members' lives are threatened, but they will recover after receiving medical treatment.	Loss of customers' or staff members' lives
Temporary or recoverable impairment of customers' or staff members' health	Permanent impairment of significant aspects of customers' or staff members' health
Safety affected	Safety violated

Step 1

Fines/Legal Penalties

Impact Type	Low Impact
Fines	Fines less than $_____are levied.
Lawsuits	Non-frivolous lawsuit or lawsuits less than $_____ are filed against the organization, or frivolous lawsuit(s) are filed against the organization.
Investigations	No queries from government or other investigative organizations
Other:	

Fines/Legal Penalties

Medium Impact	High Impact
Fines between $_____and $_____are levied.	Fines greater than $_____are levied.
Non-frivolous lawsuit or lawsuits between $_____ and $_____are filed against the organization.	Non-frivolous lawsuit or lawsuits greater than $_____ are filed against the organization.
Government or other investigative organization requests information or records (low-profile).	Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices.

Step 1

Other _____

Impact Type	Low Impact
A:	
B:	
C:	
D:	

_____	Other
Medium Impact	**High Impact**

3 Asset Identification Worksheet

		Phase 1 Process S1 Activity S1.2
Step 2	Identify information-related assets in your organization (information, systems, applications, people).	

Step 2

Information, Systems, and Applications	
System	**Information**
What systems do people in your organization need to perform their jobs?	*What information do people in your organization need to perform their jobs?*

	Information, Systems, and Applications
Applications and Services	**Other Assets**
What applications and services do people in your organization need to perform their jobs?	*What other assets are closely related to these assets?*

Step 2

Information, Systems, and Applications (cont.)

System	Information
What systems do people in your organization need to perform their jobs?	*What information do people in your organization need to perform their jobs?*

	Information, Systems, and Applications (cont.)
Applications and Services	**Other Assets**
What applications and services do people in your organization need to perform their jobs?	*What other assets are closely related to these assets?*

Step 2

People	
People	**Skills and Knowledge**
Which people have a special skill or knowledge that is vital to your organization and would be difficult to replace?	*What are their special skills or knowledge?*

	People
Related Systems	**Related Assets**
Which systems do these people use?	*Which other assets do these people use (i.e., information, services, and applications)?*

Step 2

People (cont.)	
People	**Skills and Knowledge**
Which people have a special skill or knowledge that is vital to your organization and would be difficult to replace?	*What are their special skills or knowledge?*

	People (cont.)
Related Systems	**Related Assets**
Which systems do these people use?	*Which other assets do these people use (i.e., information, services, and applications)?*

4 Security Practices Worksheet

	Phase 1 Process S1 Activity S1.3
Step 3a	Determine to what extent each practice in the survey is used by the organization.
Step 3b	As you evaluate each security practice area using the survey from Step 3a, document detailed examples of • what your organization is currently doing well in this area (security practices) • what your organization is currently *not* doing well in this area (organizational vulnerabilities)
Step 4	After completing Steps 3a and 3b, assign a stoplight status (red, green, yellow) to each security practice area. The stoplight status should reflect how well you believe your organization is performing in each area.

1. Security Awareness and Training

Step 3a

Statement	To what extent is this statement reflected in your organization?			
Staff members understand their security roles and responsibilities. This is documented and verified.	Very Much	Somewhat	Not At All	Don't Know
There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.	Very Much	Somewhat	Not At All	Don't Know
Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.	Very Much	Somewhat	Not At All	Don't Know
Staff members follow good security practice, such as • securing information for which they are responsible • not divulging sensitive information to others (resistance to social engineering) • having adequate ability to use information technology hardware and software • using good password practices • understanding and following security policies and regulations • recognizing and reporting incidents	Very Much	Somewhat	Not At All	Don't Know

1. Security Awareness and Training

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
		❑ Red ❑ Yellow ❑ Green ❑ Not Applicable

2. Security Strategy

Step 3a

Statement	To what extent is this statement reflected in your organization?			
The organization's business strategies routinely incorporate security considerations.	Very Much	Somewhat	Not At All	Don't Know
Security strategies and policies take into consideration the organization's business strategies and goals.	Very Much	Somewhat	Not At All	Don't Know
Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization.	Very Much	Somewhat	Not At All	Don't Know

2. Security Strategy

Step 3b

What is your organization currently doing well in this area?	What is your organization currently *not* doing well in this area?

Step 4

How effectively is your organization implementing the practices in this area?

- ❑ Red
- ❑ Yellow
- ❑ Green
- ❑ Not Applicable

3. Security Management

Step 3a

Statement	To what extent is this statement reflected in your organization?			
Management allocates sufficient funds and resources to information security activities.	Very Much	Somewhat	Not At All	Don't Know
Security roles and responsibilities are defined for all staff in the organization.	Very Much	Somewhat	Not At All	Don't Know
All staff at all levels of responsibility implement their assigned roles and responsibility for information security.	Very Much	Somewhat	Not At All	Don't Know
There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides.	Very Much	Somewhat	Not At All	Don't Know
The organization's hiring and termination practices for staff take information security issues into account.	Very Much	Somewhat	Not At All	Don't Know
The organization manages information security risks, including • assessing risks to information security • taking steps to mitigate information security risks	Very Much	Somewhat	Not At All	Don't Know
Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments).	Very Much	Somewhat	Not At All	Don't Know

3. Security Management

Step 3b

What is your organization currently doing well in this area?	What is your organization currently *not* doing well in this area?

Step 4

How effectively is your organization implementing the practices in this area?

- ❑ Red
- ❑ Yellow
- ❑ Green
- ❑ Not Applicable

4. Security Policies and Regulations

Step 3a

Statement	To what extent is this statement reflected in your organization?			
The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated.	Very Much	Somewhat	Not At All	Don't Know
There is a documented process for management of security policies, including • creation • administration (including periodic reviews and updates) • communication	Very Much	Somewhat	Not At All	Don't Know
The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements.	Very Much	Somewhat	Not At All	Don't Know
The organization uniformly enforces its security policies.	Very Much	Somewhat	Not At All	Don't Know

4. Security Policies and Regulations

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
		❑ Red ❑ Yellow ❑ Green ❑ Not Applicable

5. Collaborative Security Management

Step 3a

Statement	To what extent is this statement reflected in your organization?			
The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including • protecting information belonging to other organizations • understanding the security polices and procedures of external organizations • ending access to information by terminated external personnel	Very Much	Somewhat	Not At All	Don't Know
The organization documents information protection requirements and explicitly communicates them to all appropriate third parties.	Very Much	Somewhat	Not At All	Don't Know
The organization has formal mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.	Very Much	Somewhat	Not At All	Don't Know
The organization has policies and procedures for collaborating with all third-party organizations that • provide security awareness and training services • develop security policies for the organization • develop contingency plans for the organization	Very Much	Somewhat	Not At All	Don't Know

5. Collaborative Security Management

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
		❑ Red ❑ Yellow ❑ Green ❑ Not Applicable

6. Contingency Planning/Disaster Recovery

Step 3a

Statement	To what extent is this statement reflected in your organization?			
An analysis of operations, applications, and data criticality has been performed.	Very Much	Somewhat	Not At All	Don't Know
The organization has documented, reviewed, and tested • contingency plan(s) for responding to emergencies • disaster recovery plan(s) • business continuity or emergency operation plans	Very Much	Somewhat	Not At All	Don't Know
The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.	Very Much	Somewhat	Not At All	Don't Know
All staff are • aware of the contingency, disaster recovery, and business continuity plans • understand and are able to carry out their responsibilities	Very Much	Somewhat	Not At All	Don't Know

6. Contingency Planning/Disaster Recovery

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
		❑ Red ❑ Yellow ❑ Green ❑ Not Applicable

7. Physical Access Control

Step 3a

Statement	To what extent is this statement reflected in your organization?			
If staff from your organization is responsible for this area:				
Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested.	Very Much	Somewhat	Not At All	Don't Know
There are documented policies and procedures for managing visitors.	Very Much	Somewhat	Not At All	Don't Know
There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.	Very Much	Somewhat	Not At All	Don't Know
Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.	Very Much	Somewhat	Not At All	Don't Know
If staff from a third party is responsible for this area:				
The organization's requirements for physical access control are formally communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	Very Much	Somewhat	Not At All	Don't Know
The organization formally verifies that contractors and service providers have met the requirements for physical access control.	Very Much	Somewhat	Not At All	Don't Know

7. Physical Access Control

Step 3b

What is your organization currently doing well in this area?	What is your organization currently *not* doing well in this area?

Step 4

How effectively is your organization implementing the practices in this area?

- ❑ Red
- ❑ Yellow
- ❑ Green
- ❑ Not Applicable

8. Monitoring and Auditing Physical Security

Step 3a

Statement	To what extent is this statement reflected in your organization?			
If staff from your organization is responsible for this area:				
Maintenance records are kept to document the repairs and modifications of a facility's physical components.	Very Much	Somewhat	Not At All	Don't Know
An individual's or group's actions, with respect to all physically controlled media, can be accounted for.	Very Much	Somewhat	Not At All	Don't Know
Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed.	Very Much	Somewhat	Not At All	Don't Know
If staff from a third party is responsible for this area:				
The organization's requirements for monitoring physical security are formally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	Very Much	Somewhat	Not At All	Don't Know
The organization formally verifies that contractors and service providers have met the requirements for monitoring physical security.	Very Much	Somewhat	Not At All	Don't Know

8. Monitoring and Auditing Physical Security

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
		❑ Red ❑ Yellow ❑ Green ❑ Not Applicable

9. System and Network Management

Step 3a

Statement	To what extent is this statement reflected in your organization?			
If staff from your organization is responsible for this area:				
There are documented and tested security plan(s) for safeguarding the systems and networks.	Very Much	Somewhat	Not At All	Don't Know
Sensitive information is protected by secure storage (e.g., backups stored off site, discard process for sensitive information).	Very Much	Somewhat	Not At All	Don't Know
The integrity of installed software is regularly verified.	Very Much	Somewhat	Not At All	Don't Know
All systems are up to date with respect to revisions, patches, and recommendations in security advisories.	Very Much	Somewhat	Not At All	Don't Know
There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans.	Very Much	Somewhat	Not At All	Don't Know
Changes to IT hardware and software are planned, controlled, and documented.	Very Much	Somewhat	Not At All	Don't Know
IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. • Unique user identification is required for all information system users, including third-party users. • Default accounts and default passwords have been removed from systems.	Very Much	Somewhat	Not At All	Don't Know
Only necessary services are running on systems – all unnecessary services have been removed.	Very Much	Somewhat	Not At All	Don't Know
Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced.	Very Much	Somewhat	Not At All	Don't Know
If staff from a third party is responsible for this area:				
The organization's security-related system and network management requirements are formally communicated to all contractors and service providers that maintain systems and networks.	Very Much	Somewhat	Not At All	Don't Know
The organization formally verifies that contractors and service providers have met the requirements for security-related system and network management.	Very Much	Somewhat	Not At All	Don't Know

9. System and Network Management

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
		❑ Red ❑ Yellow ❑ Green ❑ Not Applicable

10. Monitoring and Auditing IT Security

Step 3a

Statement	To what extent is this statement reflected in your organization?			
If staff from your organization is responsible for this area:				
System and network monitoring and auditing tools are routinely used by the organization. Unusual activity is dealt with according to the appropriate policy or procedure.	Very Much	Somewhat	Not At All	Don't Know
Firewall and other security components are periodically audited for compliance with policy.	Very Much	Somewhat	Not At All	Don't Know
If staff from a third party is responsible for this area:				
The organization's requirements for monitoring information technology security are formally communicated to all contractors and service providers that monitor systems and networks.	Very Much	Somewhat	Not At All	Don't Know
The organization formally verifies that contractors and service providers have met the requirements for monitoring information technology security.	Very Much	Somewhat	Not At All	Don't Know

10. Monitoring and Auditing IT Security

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
		❑ Red ❑ Yellow ❑ Green ❑ Not Applicable

11. Authentication and Authorization

Step 3a

Statement	To what extent is this statement reflected in your organization?			
If staff from your organization is responsible for this area:				
Appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services, and network connections.	Very Much	Somewhat	Not At All	Don't Know
There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.	Very Much	Somewhat	Not At All	Don't Know
Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner. Methods or mechanisms are periodically reviewed and verified.	Very Much	Somewhat	Not At All	Don't Know
If staff from a third party is responsible for this area:				
The organization's requirements for controlling access to systems and information are formally communicated to all contractors and service providers that provide authentication and authorization services.	Very Much	Somewhat	Not At All	Don't Know
The organization formally verifies that contractors and service providers have met the requirements for authentication and authorization.	Very Much	Somewhat	Not At All	Don't Know

11. Authentication and Authorization

Step 3b

What is your organization currently doing well in this area?	What is your organization currently *not* doing well in this area?

Step 4

How effectively is your organization implementing the practices in this area?

- ❑ Red
- ❑ Yellow
- ❑ Green
- ❑ Not Applicable

12. Vulnerability Management

Step 3a

Statement	To what extent is this statement reflected in your organization?			
If staff from your organization is responsible for this area:				
There is a documented set of procedures for managing vulnerabilities, including • selecting vulnerability evaluation tools, checklists, and scripts • keeping up to date with known vulnerability types and attack methods • reviewing sources of information on vulnerability announcements, security alerts, and notices • identifying infrastructure components to be evaluated • scheduling of vulnerability evaluations • interpreting and responding to the evaluation results • maintaining secure storage and disposition of vulnerability data	Very Much	Somewhat	Not At All	Don't Know
Vulnerability management procedures are followed and are periodically reviewed and updated.	Very Much	Somewhat	Not At All	Don't Know
Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.	Very Much	Somewhat	Not At All	Don't Know
If staff from a third party is responsible for this area:				
The organization's vulnerability management requirements are formally communicated to all contractors and service providers that manage technology vulnerabilities.	Very Much	Somewhat	Not At All	Don't Know
The organization formally verifies that contractors and service providers have met the requirements for vulnerability management.	Very Much	Somewhat	Not At All	Don't Know

12. Vulnerability Management

Step 3b

What is your organization currently doing well in this area?	What is your organization currently *not* doing well in this area?

Step 4

How effectively is your organization implementing the practices in this area?

- ❑ Red
- ❑ Yellow
- ❑ Green
- ❑ Not Applicable

13. Encryption

Step 3a

Statement	To what extent is this statement reflected in your organization?			
If staff from your organization is responsible for this area:				
Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g., data encryption, public key infrastructure, virtual private network technology).	Very Much	Somewhat	Not At All	Don't Know
Encrypted protocols are used when remotely managing systems, routers, and firewalls.	Very Much	Somewhat	Not At All	Don't Know
If staff from a third party is responsible for this area:				
The organization's requirements for protecting sensitive information are formally communicated to all contractors and service providers that provide encryption technologies.	Very Much	Somewhat	Not At All	Don't Know
The organization formally verifies that contractors and service providers have met the requirements for implementing encryption technologies.	Very Much	Somewhat	Not At All	Don't Know

13. Encryption

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
		❑ Red ❑ Yellow ❑ Green ❑ Not Applicable

14. Security Architecture and Design

Step 3a

Statement	To what extent is this statement reflected in your organization?			
If staff from your organization is responsible for this area:				
System architecture and design for new and revised systems include considerations for • security strategies, policies, and procedures • history of security compromises • results of security risk assessments	Very Much	Somewhat	Not At All	Don't Know
The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.	Very Much	Somewhat	Not At All	Don't Know
If staff from a third party is responsible for this area:				
The organization's security-related requirements are formally communicated to all contractors and service providers that design systems and networks.	Very Much	Somewhat	Not At All	Don't Know
The organization formally verifies that contractors and service providers have met the requirements for security architecture and design.	Very Much	Somewhat	Not At All	Don't Know

14. Security Architecture and Design

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
		❑ Red ❑ Yellow ❑ Green ❑ Not Applicable

15. Incident Management

Step 3a

Statement	To what extent is this statement reflected in your organization?			
If staff from your organization is responsible for this area:				
Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations.	Very Much	Somewhat	Not At All	Don't Know
Incident management procedures are periodically tested, verified, and updated.	Very Much	Somewhat	Not At All	Don't Know
There are documented policies and procedures for working with law enforcement agencies.	Very Much	Somewhat	Not At All	Don't Know
If staff from a third party is responsible for this area:				
The organization's requirements for managing incidents are formally communicated to all contractors and service providers that provide incident management services.	Very Much	Somewhat	Not At All	Don't Know
The organization formally verifies that contractors and service providers have met the requirements for managing incidents.	Very Much	Somewhat	Not At All	Don't Know

15. Incident Management

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
		❑ Red ❑ Yellow ❑ Green ❑ Not Applicable

5 Critical Asset Selection Worksheet

	Phase 1 Process S2 Activity S2.1
Step 5	Review the information-related assets that you identified during Step 2 and select up to five (5) assets that are most critical to the organization.

Step 5

Questions to Consider:	*Which assets would have a large adverse impact on the organization if* • *they are disclosed to unauthorized people?* • *they are modified without authorization?* • *they are lost or destroyed?* • *access to them is interrupted?*

Critical Asset
1.
2.
3.
4.
5.

Notes

6 Infrastructure Review Worksheet

	Phase 2 Process S3 Activity S3.2
Step 19a	Document the classes of components that are related to one or more critical assets and that can provide access to those assets. Mark the path to each class selected in Steps 18a-18e. Note any relevant subclasses or specific examples when appropriate.
Step 19b	For each class of components documented in Step 19a, note which critical assets are related to that class.
Step 20	For each class of components documented in Step 19a, note the person or group responsible for maintaining and securing that class of component.
Step 21	For each class of components documented in Step 19a, note the extent to which security is considered when configuring and maintaining that class. Also record how you came to that conclusion. Finally, document any additional context relevant to your infrastructure review.
Gap Analysis	Refine Phase 1 information based on the analysis of access paths and technology-related processes. Update the following, if appropriate: • Mark any additional branches of the threat trees when appropriate (Step 12). Be sure to document appropriate context for each branch you mark (Steps 13-16). • Revise documented areas of concern by adding additional details when appropriate. Identify and document new areas of concern when appropriate (Step 16). • Revise documented security practices and organizational vulnerabilities by adding additional details when appropriate. Identify and document new security practices and/or organizational vulnerabilities when appropriate (Step 3b). • Revise the stoplight status for a security practice when appropriate (Step 4).

Note
In Step 19a, mark the path to each class selected in Steps 18a-18e.

Step 19a	Step 19b					Step 20
Class	**Critical Assets**					**Responsibility**
Which classes of components are related to one or more critical assets?	*Which critical assets are related to each class?*					*Who is responsible for maintaining and securing each class of components?*
(Document any relevant subclasses or specific examples when appropriate.)	1.	2.	3.	4.	5.	
Servers						
Internal Networks						
On-Site Workstations						
Laptops						
PDAs/Wireless Components						

Step 21

Protection		Notes/Issues
To what extent is security considered when configuring and maintaining each class of components?	*How do you know?*	*What additional information do you want to record?*

Very Much	Somewhat	Not At All	Don't Know	Formal Techniques	Informal Means	Other	
Servers							
		❑		❑	❑	❑	
		❑		❑	❑	❑	
		❑		❑	❑	❑	
Internal Networks							
		❑		❑	❑	❑	
		❑		❑	❑	❑	
		❑		❑	❑	❑	
On-Site Workstations							
		❑		❑	❑	❑	
		❑		❑	❑	❑	
		❑		❑	❑	❑	
Laptops							
		❑		❑	❑	❑	
		❑		❑	❑	❑	
		❑		❑	❑	❑	
PDAs/Wireless Components							
		❑		❑	❑	❑	
		❑		❑	❑	❑	
		❑		❑	❑	❑	

Note
In Step 19a, mark the path to each class selected in Steps 18a-18e.

Step 19a	Step 19b					Step 20
Class	**Critical Assets**					**Responsibility**
Which classes of components are related to one or more critical assets?	*Which critical assets are related to each class?*					*Who is responsible for maintaining and securing each class of components?*
(Document any relevant subclasses or specific examples when appropriate.)	1.	2.	3.	4.	5.	
Other Systems						
Storage Devices						
External Networks						
Home/External Workstations						
Other _____						

Step 21

Protection		Notes/Issues
To what extent is security considered when configuring and maintaining each class of components?	*How do you know?*	*What additional information do you want to record?*

Very Much	Somewhat	Not At All	Don't Know	Formal Techniques	Informal Means	Other	
Other Systems							
|----------|----------|	❑	❑	❑	❑		
|----------|----------|	❑	❑	❑	❑		
|----------|----------|	❑	❑	❑	❑		
Storage Devices							
|----------|----------|	❑	❑	❑	❑		
|----------|----------|	❑	❑	❑	❑		
|----------|----------|	❑	❑	❑	❑		
External Networks							
|----------|----------|	❑	❑	❑	❑		
|----------|----------|	❑	❑	❑	❑		
|----------|----------|	❑	❑	❑	❑		
Home/External Workstations							
|----------|----------|	❑	❑	❑	❑		
|----------|----------|	❑	❑	❑	❑		
|----------|----------|	❑	❑	❑	❑		
Other _____							
|----------|----------|	❑	❑	❑	❑		
|----------|----------|	❑	❑	❑	❑		
|----------|----------|	❑	❑	❑	❑		

7 Probability Evaluation Criteria Worksheet

	Phase 3 Process S4 Activity S4.2
Step 23	Define a qualitative set of measures (high, medium, low) against which you will evaluate the likelihood of a threat occurring.

Step 23

Frequency-Based Criteria

1. *Think about what constitutes a high, medium, and low likelihood of occurrence for threats to your organization's critical assets.*

Time Between Events	Daily	Weekly	Monthly	Four Times Per Year	Two Times Per Year
Annualized Frequency	365	52	12	4	2

2. *Draw lines that separate high from medium and medium from low.*

One Time Per Year	Once Every Two Years	Once Every Five Years	Once Every 10 Years	Once Every 20 Years	Once Every 50 Years
1	0.5	0.2	0.1	0.05	0.02

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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

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

6. AUTHOR(S)

Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody

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

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

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

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

14. SUBJECT TERMS	15. NUMBER OF PAGES
information security, risk management, OCTAVE	74

16. PRICE CODE

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

OCTAVE®-S Implementation Guide, Version 1

Volume 5: Critical Asset Worksheets for Information

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

HANDBOOK
CMU/SEI-2003-HB-003

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

OCTAVE®-S Implementation Guide, Version 1

Volume 5: Critical Asset Worksheets for Information

CMU/SEI-2003-HB-003

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

Networked Systems Survivability Program

This report was prepared for the

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

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

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

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

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

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

Table of Contents

List of Tables

About This Document

This document is Volume 5 of the *OCTAVE-S Implementation Guide*, a 10-volume handbook supporting the OCTAVE-S methodology. This volume provides worksheets to document data related to critical assets that are categorized as information.

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℠ (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 Introduction

This document contains the Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE®)-S worksheets related to critical assets that are information. The activities related to these worksheets are focused on analyzing a critical asset.

Table 1 provides a brief introduction to the contents of this workbook, using step numbers as a key. For more details about how to complete each step, refer to the *OCTAVE®-S Method Guidelines*, which can be found in Volume 3 of the *OCTAVE®-S Implementation Guide*.

Table 1: Worksheets Provided in This Workbook

Step	Description	Worksheet	Activity	Pages
Step 6	Start a *Critical Asset Information worksheet* for each critical asset. Record the name of the critical asset on its *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 7	Record your rationale for selecting each critical asset on that asset's *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 8	Record a description for each critical asset on that asset's *Critical Asset Selection worksheet*. Consider who uses each critical asset as well as who is responsible for it.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 9	Record assets that are related to each critical asset on that asset's *Critical Asset Information worksheet*. Refer to the *Asset Identification worksheet* to determine which assets are related to each critical asset.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8

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

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

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 10	Record the security requirements for each critical asset on that asset's *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 11	For each critical asset, record the most important security requirement on that asset's *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 12	Complete all appropriate threat trees for each critical asset. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on any threat tree, review the description and examples of that threat in the *Threat Translation Guide*.	Risk Profile Threat Translation Guide	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-54
Step 13	Record specific examples of threat actors on the *Risk Profile worksheet* for each applicable actor-motive combination.	Risk Profile	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-54
Step 14	Record the strength of the motive for deliberate threats due to human actors. Also record how confident you are in your estimate of the strength of the actor's motive.	Risk Profile	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-54
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.	Risk Profile	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-54
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.	Risk Profile	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-54

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 17	Select the system of interest for each critical asset (i.e., the system most closely related to the critical asset).	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58
Step 18a	Review paths used to access each critical asset, and select key classes of components related to each critical asset. Determine which classes of components are part of the system of interest.	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58
Step 18b	Determine which classes of components serve as intermediate access points (i.e., which components are used to transmit information and applications from the system of interest to people).	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58
Step 18c	Determine which classes of components, both internal and external to the organization's networks, are used by people (e.g., users, attackers) to access the system.	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58
Step 18d	Determine where information from the system of interest is stored for backup purposes.	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58
Step 18e	Determine which other systems access information or applications from the system of interest and which other classes of components can be used to access critical information or services from the system of interest.	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) for each active threat to each critical asset.	Risk Profile Impact Evaluation Criteria	Phase 3 Process S4 S4.1 Evaluate Impacts of Threats	9-54
Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) for each active threat to each critical asset. Document your confidence level in your probability estimate.	Risk Profile Probability Evaluation Criteria	Phase 3 Process S4 S4.3 Evaluate Probabilities of Threats	9-54
Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of each critical asset's *Risk Profile worksheet*.	Risk Profile Security Practices	Phase 3 Process S5 S5.2 Select Mitigation Approaches	9-54
Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.	Risk Profile	Phase 3 Process S5 S5.2 Select Mitigation Approaches	9-54

2 Critical Asset Information Worksheet for Information

Phase 1
Process S2
Activity S2.1

Step 6	Start a *Critical Asset Information worksheet* for each critical asset. Record the name of the critical asset on its *Critical Asset Information worksheet*.
Step 7	Record your rationale for selecting each critical asset on that asset's *Critical Asset Information worksheet*.
Step 8	Record a description for each critical asset on that asset's *Critical Asset Selection worksheet*. Consider who uses each critical asset as well as who is responsible for it.
Step 9	Record assets that are related to each critical asset on that asset's *Critical Asset Information worksheet*. Refer to the *Asset Identification worksheet* to determine which assets are related to each critical asset.

Phase 1
Process S2
Activity S2.2

Step 10	Record the security requirements for each critical asset on that asset's *Critical Asset Information worksheet*.
Step 11	For each critical asset, record the most important security requirement on that asset's *Critical Asset Information worksheet*.

Step 6	Step 7
Critical Asset	**Rationale for Selection**
What is the critical information?	*Why is this information critical to the organization?*

Step 9
Related Assets
Which assets are related to this information?
Systems: Applications:
Other:

Step 8

Description	
Who uses the information?	*Who is responsible for the information?*

Step 10

Security Requirements		**Step 11** **Most Important Security Requirement**
What are the security requirements for this information? *(Hint: Focus on what the security requirements should be for this information, not what they currently are.)*		*Which security requirement is most important for this information?*
❑ Confidentiality	Only authorized personnel can view _____.	❑ Confidentiality
❑ Integrity	Only authorized personnel can modify _____.	❑ Integrity ❑ Availability ❑ Other
❑ Availability	_____ must be available for personnel to perform their jobs. Unavailability cannot exceed _____ hour(s) per every _____ hours.	
❑ Other	_____ _____	

3 Risk Profile Worksheet for Information – Human Actors Using Network Access

Phase 1
Process S2
Activity S2.3

Step 12	Complete the threat tree for *human actors using network access*. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on the threat tree, review the description and examples of that threat in the *Threat Translation Guide* (see pp. 60-63 of this workbook).
Step 13	Record specific examples of threat actors on the *Risk Profile worksheet* for each applicable actor-motive combination.
Step 14	Record the strength of the motive for deliberate threats due to human actors. Also record how confident you are in your estimate of the strength of the actor's motive.
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.

continued

Phase 3
Process S4
Activity S4.1

Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) to each active threat.

Phase 3
Process S4
Activity S4.3

Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) to each active threat. Document your confidence level in your probability estimate.

Phase 3
Process S5
Activity S5.2

Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of the following worksheet.

Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.

Human Actors Using Network Access **Basic Risk Profile**

Step 12

Threat

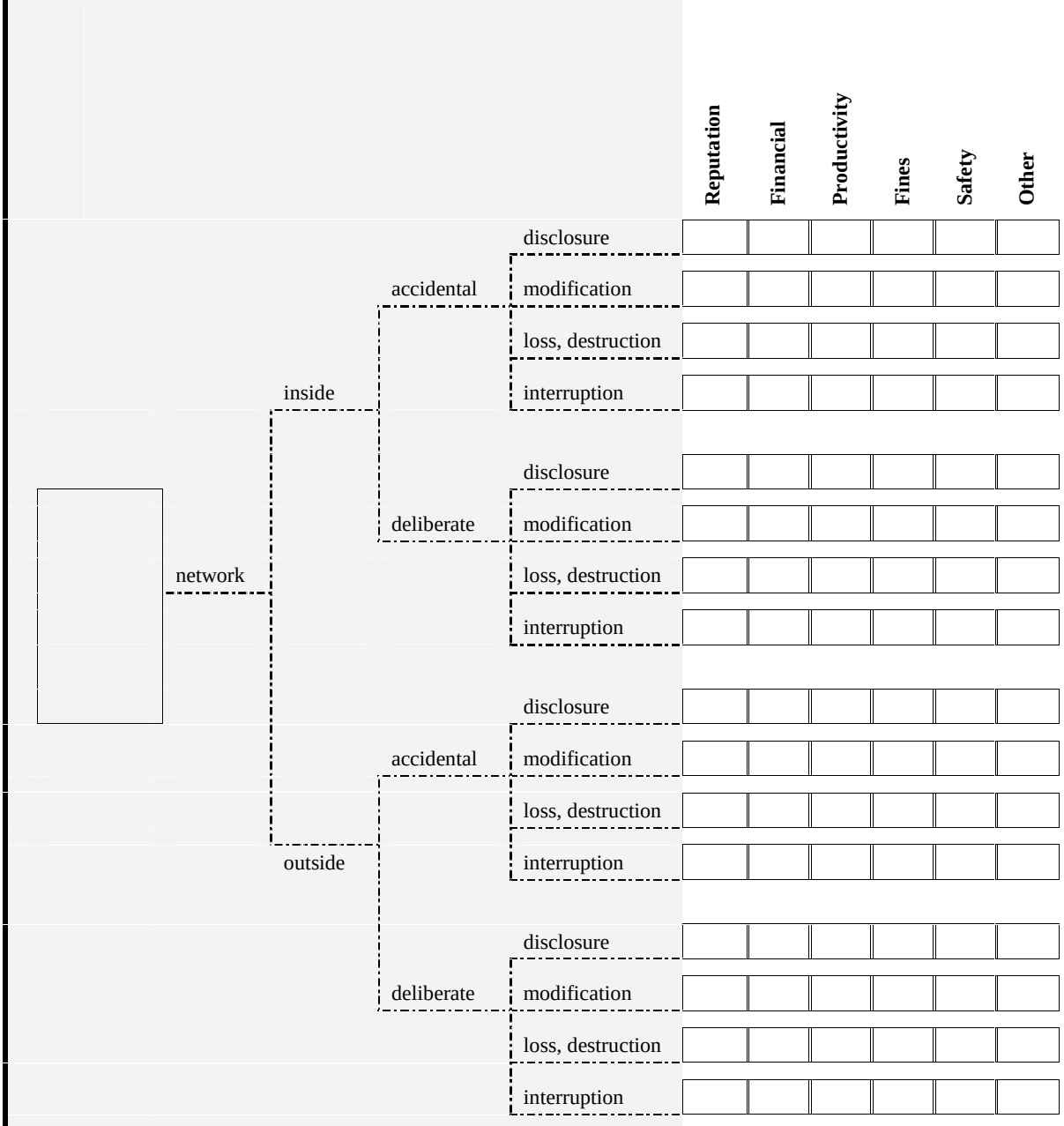
For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Step 22

Impact Values

What is the potential impact on the organization in each applicable area?



Basic Risk Profile | **Human Actors Using Network Access**

Step 24

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value	Confidence	
	Very	
	Somewhat	
	Not At All	

Step 26

Security Practice Areas

What is the stoplight status for each security practice area?

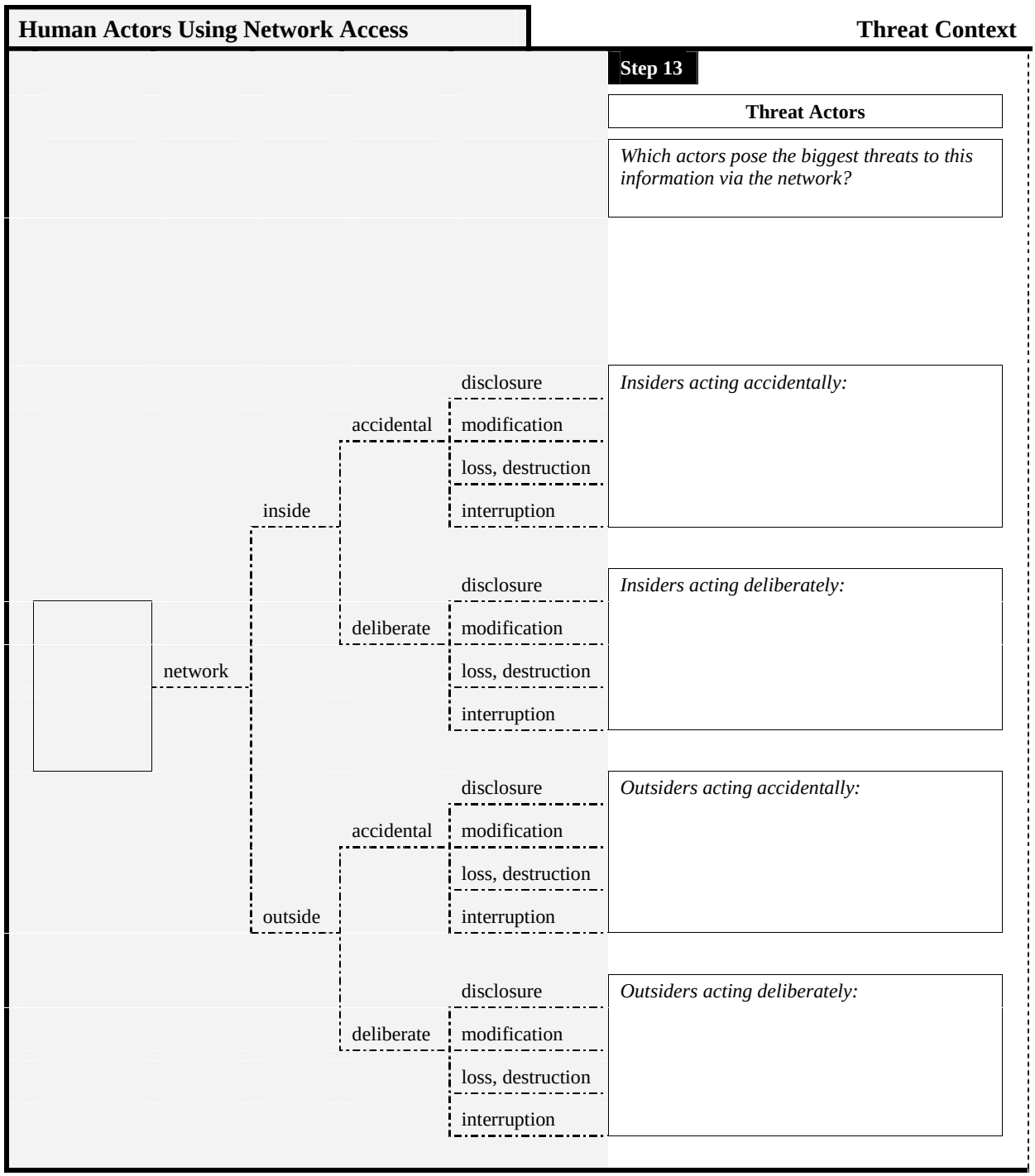
Strategic						Operational								
1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt

Step 27

Approach

What is your approach for addressing each risk?

Accept	Defer	Mitigate
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑


Human Actors Using Network Access
Threat Context
Step 13
Threat Actors
Which actors pose the biggest threats to this information via the network?
network
inside
outside
accidental
deliberate
disclosure
modification
loss, destruction
interruption
Insiders acting accidentally:
Insiders acting deliberately:
Outsiders acting accidentally:
Outsiders acting deliberately:

Threat Context | **Human Actors Using Network Access**

Step 14 | **Step 15**

Motive						History			
How strong is the actor's motive?			*How confident are you in this estimate?*			*How often has this threat occurred in the past?*	*How accurate are the data?*		
High	**Medium**	**Low**	**Very**	**Somewhat**	**Not At All**		**Very**	**Somewhat**	**Not At All**
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑

Step 16

Human Actors Using Network Access	Areas of Concern

Insiders Using Network Access

Give examples of how *insiders acting accidentally* could use network access to threaten this information.	
Give examples of how *insiders acting deliberately* could use network access to threaten this information.	

Outsiders Using Network Access

Give examples of how *outsiders acting accidentally* could use network access to threaten this information.	
Give examples of how *outsiders acting deliberately* could use network access to threaten this information.	

Areas of Concern

Insiders Using Network Access

Outsiders Using Network Access

4 Risk Profile Worksheet for Information – Human Actors Using Physical Access

Phase 1
Process S2
Activity S2.3

Step 12	Complete the threat tree for *human actors using physical access*. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on the threat tree, review the description and examples of that threat in the *Threat Translation Guide* (see pp. 64-67 of this workbook).
Step 13	Record specific examples of threat actors on the *Risk Profile worksheet* for each applicable actor-motive combination.
Step 14	Record the strength of the motive for deliberate threats due to human actors. Also record how confident you are in your estimate of the strength of the actor's motive.
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.

continued

	Phase 3 **Process S4** **Activity S4.1**
Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) to each active threat.

	Phase 3 **Process S4** **Activity S4.3**
Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) to each active threat. Document your confidence level in your probability estimate.

	Phase 3 **Process S5** **Activity S5.2**
Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of the following worksheet.

Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.

Human Actors Using Physical Access | **Basic Risk Profile**

Step 12

Threat

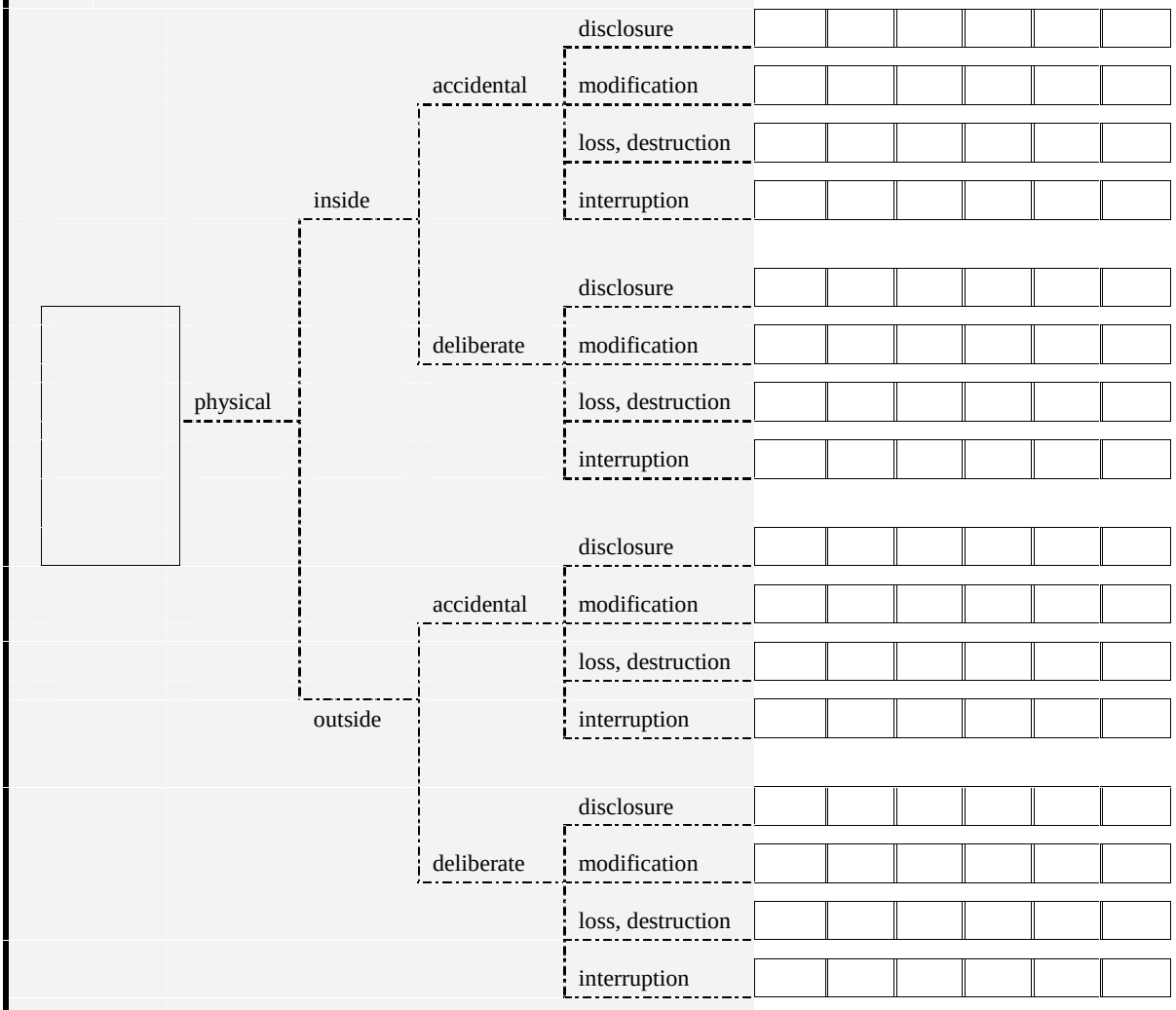
For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Step 22

Impact Values

What is the potential impact on the organization in each applicable area?



Basic Risk Profile | **Human Actors Using Physical Access**

Step 24

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value	Confidence: Very	Somewhat	Not At All

Step 26

Security Practice Areas

What is the stoplight status for each security practice area?

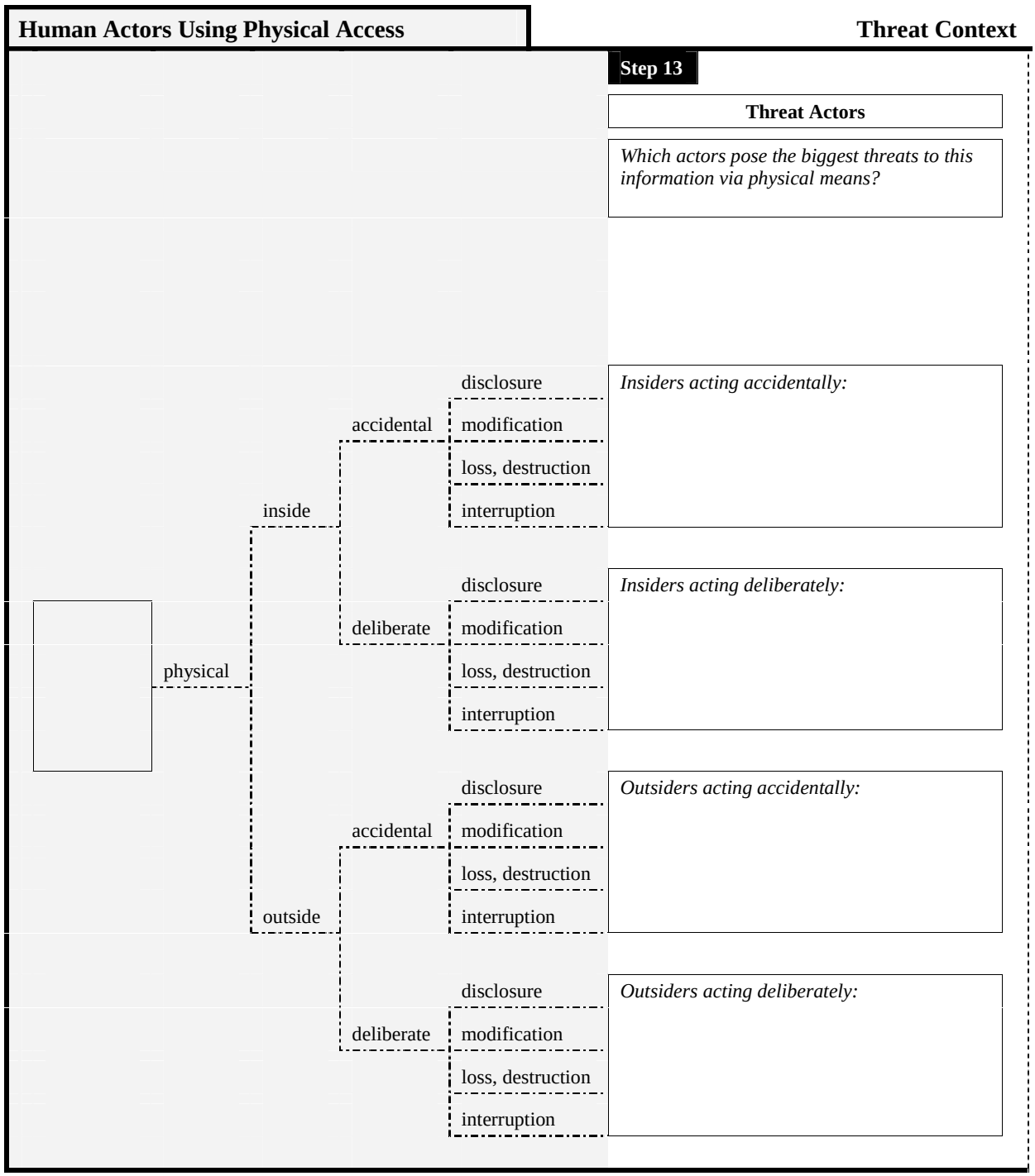
Strategic						Operational								
1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt

Step 27

Approach

What is your approach for addressing each risk?

Accept	Defer	Mitigate
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑


Human Actors Using Physical Access
Threat Context
Step 13
Threat Actors
Which actors pose the biggest threats to this information via physical means?
physical
inside
outside
accidental
deliberate
disclosure
modification
loss, destruction
interruption
Insiders acting accidentally:
Insiders acting deliberately:
Outsiders acting accidentally:
Outsiders acting deliberately:

Threat Context | **Human Actors Using Physical Access**

Step 14 | **Step 15**

Motive						History			
How strong is the actor's motive?			*How confident are you in this estimate?*			*How often has this threat occurred in the past?*	*How accurate are the data?*		
High	**Medium**	**Low**	**Very**	**Somewhat**	**Not At All**		**Very**	**Somewhat**	**Not At All**
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑

Step 16

Human Actors Using Physical Access	Areas of Concern

Insiders Using Physical Access

Give examples of how *insiders acting accidentally* could use physical access to threaten this information.	
Give examples of how *insiders acting deliberately* could use physical access to threaten this information.	

Outsiders Using Physical Access

Give examples of how *outsiders acting accidentally* could use physical access to threaten this information.	
Give examples of how *outsiders acting deliberately* could use physical access to threaten this information.	

Areas of Concern

Insiders Using Physical Access

Outsiders Using Physical Access

5 Risk Profile Worksheet for Information – System Problems

Phase 1
Process S2
Activity S2.3

Step 12	Complete the threat tree for *system problems*. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on the threat tree, review the description and examples of that threat in the *Threat Translation Guide* (see pp. 68-71 of this workbook).
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.

continued

	Phase 3 Process S4 Activity S4.1
Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) to each active threat.

	Phase 3 Process S4 Activity S4.3
Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) to each active threat. Document your confidence level in your probability estimate.

	Phase 3 Process S5 Activity S5.2
Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of the following worksheet.

Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.

System Problems | **Basic Risk Profile**

Step 12 | **Step 22**

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Impact Values

What is the potential impact on the organization in each applicable area?

Asset	Actor	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other
	software defects	disclosure						
		modification						
		loss, destruction						
		interruption						
	system crashes	disclosure						
		modification						
		loss, destruction						
		interruption						
	hardware defects	disclosure						
		modification						
		loss, destruction						
		interruption						
	malicious code (virus, worm, Trojan horse, back door)	disclosure						
		modification						
		loss, destruction						
		interruption						

Basic Risk Profile | **System Problems**

Step 24

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value	Confidence	
	Very	
	Somewhat	
	Not At All	

Step 26

Security Practice Areas

What is the stoplight status for each security practice area?

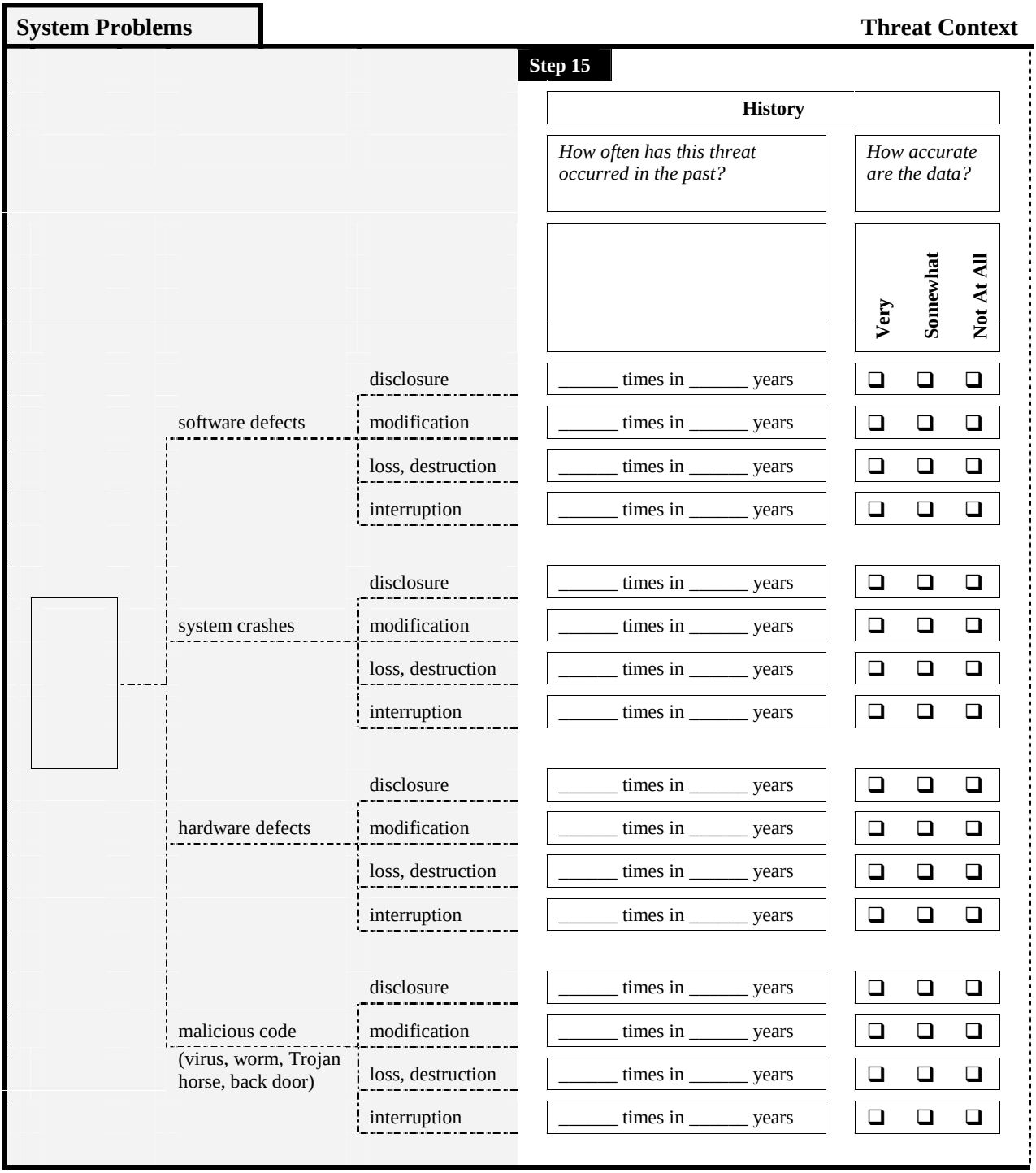
Value	Confidence	Strategic						Operational								
		1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt
	Very															
	Somewhat															
	Not At All															
	|--------|--------|																
	|--------|--------|																
	|--------|--------|																
	|--------|--------|																
	|--------|--------|																
	|--------|--------|																
	|--------|--------|																
	|--------|--------|																
	|--------|--------|																
	|--------|--------|																
	|--------|--------|																
	|--------|--------|																
	|--------|--------|																
	|--------|--------|																
	|--------|--------|																
	|--------|--------|																

Step 27

Approach

What is your approach for addressing each risk?

Accept	Defer	Mitigate
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑


System Problems
Threat Context
Step 15
History
How often has this threat occurred in the past?
How accurate are the data?
Very
Somewhat
Not At All
software defects
system crashes
hardware defects
malicious code
(virus, worm, Trojan horse, back door)
disclosure
modification
loss, destruction
interruption
_____ times in _____ years

Threat Context	System Problems

Notes
What additional notes about each threat do you want to record?

Step 16

System Problems	Areas of Concern
Software Defects	
Give examples of how *software defects* could threaten this information.	
System Crashes	
Give examples of how *system crashes* could threaten this information.	
Hardware Defects	
Give examples of how *hardware defects* could threaten this information.	
Malicious Code	
Give examples of how *malicious code* could threaten this information. (Consider viruses, worms, Trojan horses, back doors, others)	

Areas of Concern

	Software Defects
	System Crashes
	Hardware Defects
	Malicious Code

6 Risk Profile Worksheet for Information – Other Problems

Phase 1
Process S2
Activity S2.3

Step 12	Complete the threat tree for *other problems*. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on the threat tree, review the description and examples of that threat in the *Threat Translation Guide* (see pp. 72-77 of this workbook).
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.

continued

	Phase 3 **Process S4** **Activity S4.1**
Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) to each active threat.

	Phase 3 **Process S4** **Activity S4.3**
Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) to each active threat. Document your confidence level in your probability estimate.

	Phase 3 **Process S5** **Activity S5.2**
Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of the following worksheet.

Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.

Other Problems | **Basic Risk Profile**

Step 12

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Step 22

Impact Values

What is the potential impact on the organization in each applicable area?

Asset	Actor	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other
	power supply problems	disclosure						
		modification						
		loss, destruction						
		interruption						
	telecommunications problems or unavailability	disclosure						
		modification						
		loss, destruction						
		interruption						
	third-party problems or unavailability of third-party systems	disclosure						
		modification						
		loss, destruction						
		interruption						
	natural disasters (e.g., flood, fire, tornado)	disclosure						
		modification						
		loss, destruction						
		interruption						

Basic Risk Profile | **Other Problems**

Step 24 | **Step 26** | **Step 27**

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value **Confidence**

	Very	Somewhat	Not At All
		|--------|--------|	
		|--------|--------|	
		|--------|--------|	
		|--------|--------|	
		|--------|--------|	
		|--------|--------|	
		|--------|--------|	
		|--------|--------|	
		|--------|--------|	
		|--------|--------|	
		|--------|--------|	
		|--------|--------|	
		|--------|--------|	
		|--------|--------|	
		|--------|--------|	

Security Practice Areas

What is the stoplight status for each security practice area?

	Strategic						Operational								
	1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt

Approach

What is your approach for addressing each risk?

Accept	Defer	Mitigate
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑

Other Problems

Threat Context

Step 15

			History			
			How often has this threat occurred in the past?	*How accurate are the data?*		
				Very	**Somewhat**	**Not At All**
		disclosure	_____ times in _____ years	❑	❑	❑
	power supply	modification	_____ times in _____ years	❑	❑	❑
	problems	loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑
		disclosure	_____ times in _____ years	❑	❑	❑
	telecommunications	modification	_____ times in _____ years	❑	❑	❑
	problems or unavailability	loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑
		disclosure	_____ times in _____ years	❑	❑	❑
	third-party problems	modification	_____ times in _____ years	❑	❑	❑
	or unavailability of third-party systems	loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑
		disclosure	_____ times in _____ years	❑	❑	❑
	natural disasters	modification	_____ times in _____ years	❑	❑	❑
	(e.g., flood, fire, tornado)	loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑

Threat Context	Other Problems

Notes
What additional notes about each threat do you want to record?

Step 16

Other Problems	Areas of Concern
Power Supply Problems	
Give examples of how *power supply problems* could threaten this information.	
Telecommunications Problems	
Give examples of how *telecommunications problems* could threaten this information.	
Third-Party Problems	
Give examples of how *third-party problems* could threaten this information.	
Natural Disasters	
Give examples of how *natural disasters* could threaten this information.	

Areas of Concern

Power Supply Problems
Telecommunications Problems
Third-Party Problems
Natural Disasters

Other Problems (cont.) **Basic Risk Profile**

Step 12

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Step 22

Impact Values

What is the potential impact on the organization in each applicable area?

Asset	Actor	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other
	physical configuration or arrangement of buildings, offices, or equipment	disclosure						
		modification						
		loss, destruction						
		interruption						
		disclosure						
		modification						
		loss, destruction						
		interruption						
		disclosure						
		modification						
		loss, destruction						
		interruption						
		disclosure						
		modification						
		loss, destruction						
		interruption						

Basic Risk Profile | **Other Problems (cont.)**

Step 24 | **Step 26** | **Step 27**

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value **Confidence**

Security Practice Areas

What is the stoplight status for each security practice area?

Strategic | **Operational**

Approach

What is your approach for addressing each risk?

Value	Confidence	1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt	Accept	Defer	Mitigate
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑

Other Problems (cont.)

Threat Context

Step 15

			History			
			How often has this threat occurred in the past?	*How accurate are the data?*		
				Very	**Somewhat**	**Not At All**
		disclosure	_____ times in _____ years	❑	❑	❑
	physical configuration	modification	_____ times in _____ years	❑	❑	❑
	or arrangement of buildings, offices, or equipment	loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑
		disclosure	_____ times in _____ years	❑	❑	❑
		modification	_____ times in _____ years	❑	❑	❑
		loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑
		disclosure	_____ times in _____ years	❑	❑	❑
		modification	_____ times in _____ years	❑	❑	❑
		loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑
		disclosure	_____ times in _____ years	❑	❑	❑
		modification	_____ times in _____ years	❑	❑	❑
		loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑

Threat Context | **Other Problems (cont.)**

Notes
What additional notes about each threat do you want to record?

Step 16

Other Problems (cont.)	**Areas of Concern**
Physical Configuration Problems	
Give examples of how *physical configuration of buildings, offices, or equipment* could threaten this information.	
Give examples of how _____ could threaten this information.	
Give examples of how _____ could threaten this information.	
Give examples of how _____ could threaten this information.	

Areas of Concern

	Physical Configuration Problems

7 Network Access Paths Worksheet

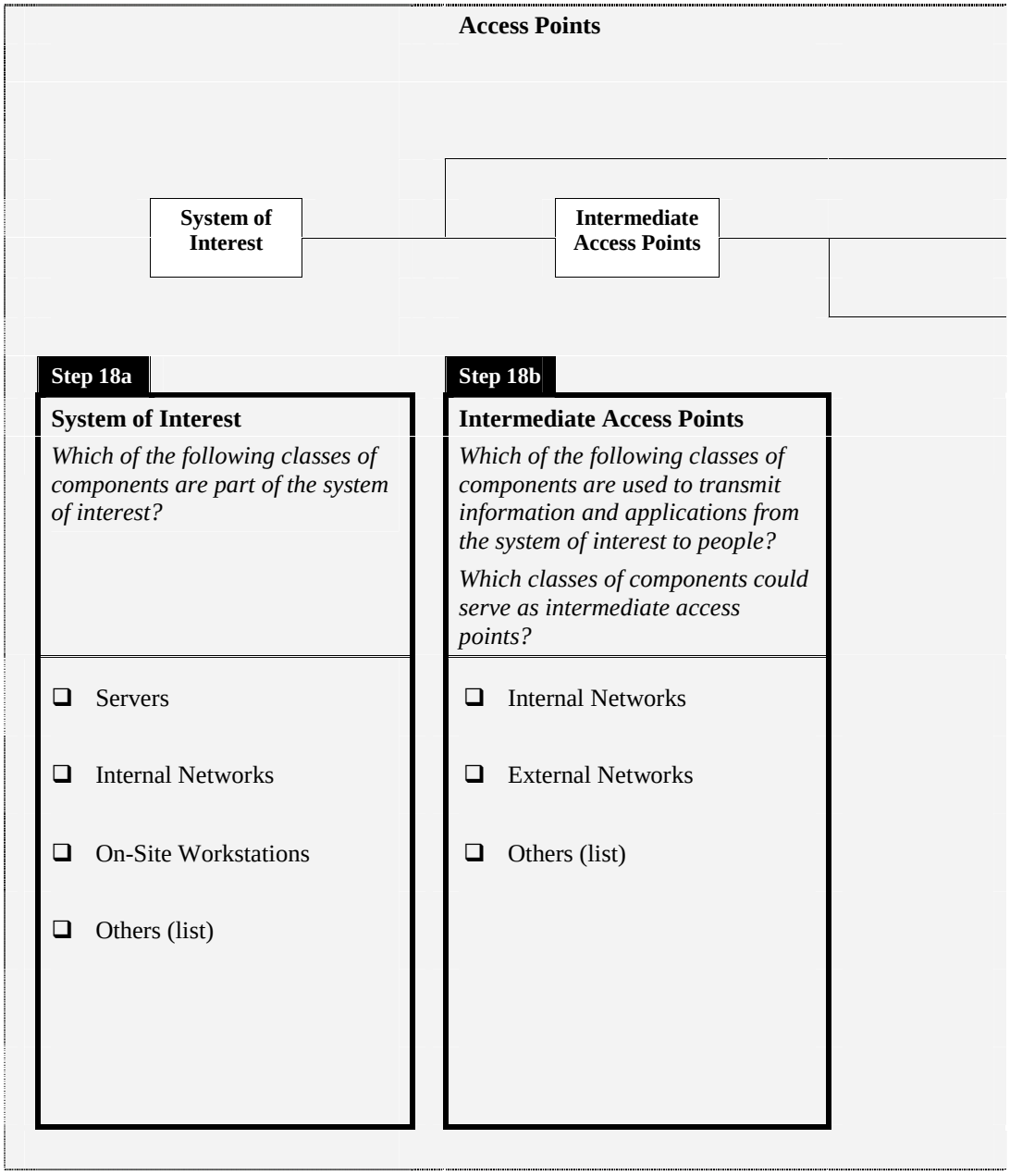
Phase 2
Process S3
Activity S3.1

Step 17	Select the system of interest for each critical asset (i.e., the system most closely related to the critical asset).
Step 18a	Review paths used to access each critical asset, and select key classes of components related to each critical asset. Determine which classes of components are part of the system of interest.
Step 18b	Determine which classes of components serve as intermediate access points (i.e., which components are used to transmit information and applications from the system of interest to people).
Step 18c	Determine which classes of components, both internal and external to the organization's networks, are used by people (e.g., users, attackers) to access the system.
Step 18d	Determine where information from the system of interest is stored for backup purposes.
Step 18e	Determine which other systems access information or applications from the system of interest and which other classes of components can be used to access critical information or services from the system of interest.

Step 17

System of Interest

What system or systems are most closely related to the critical asset?



Step 18a

System of Interest

Which of the following classes of components are part of the system of interest?

- ❑ Servers
- ❑ Internal Networks
- ❑ On-Site Workstations
- ❑ Others (list)

Step 18b

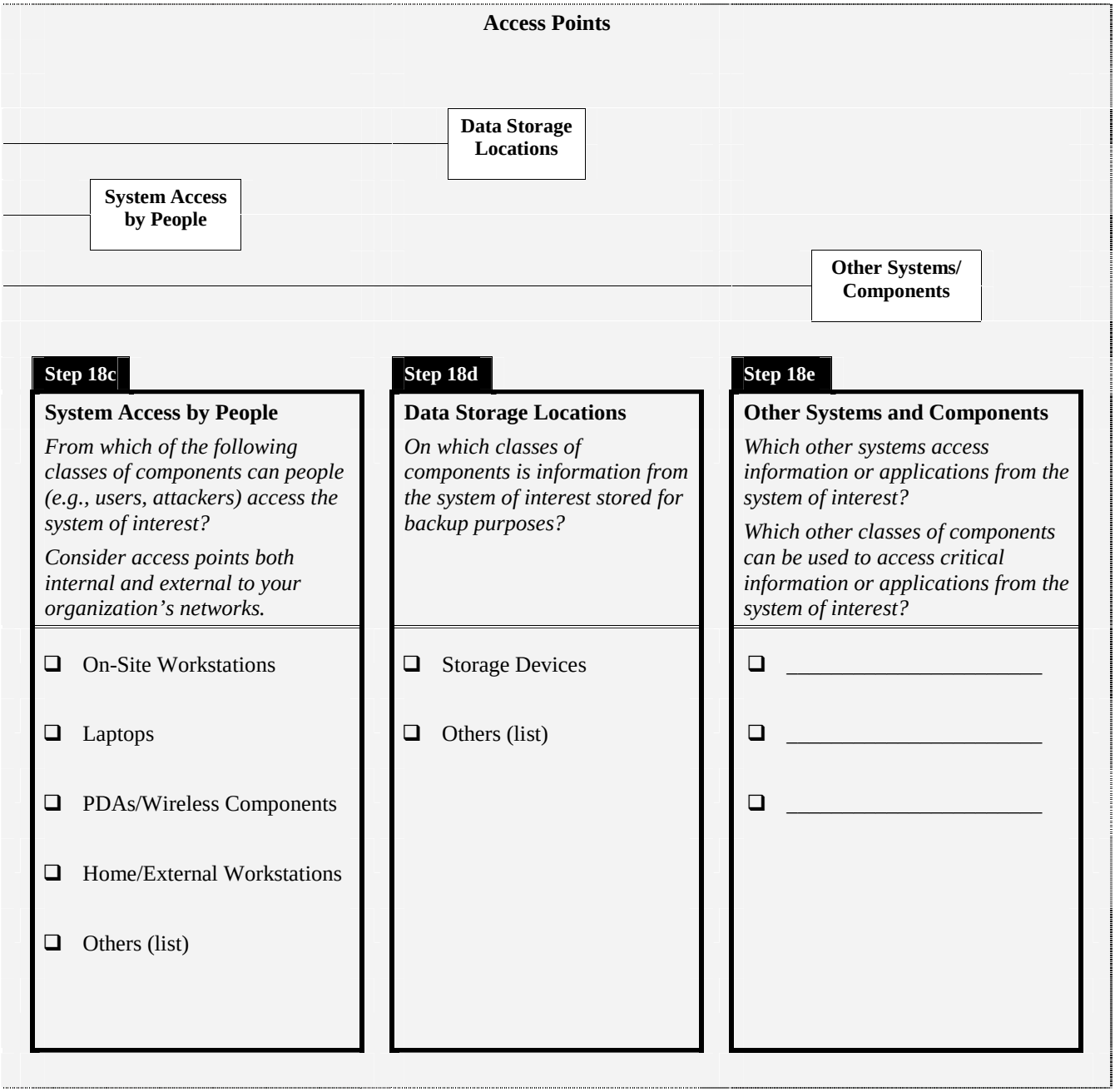
Intermediate Access Points

Which of the following classes of components are used to transmit information and applications from the system of interest to people?

Which classes of components could serve as intermediate access points?

- ❑ Internal Networks
- ❑ External Networks
- ❑ Others (list)

***Note**: When you select a key class of components, make sure that you also document any relevant subclasses or specific examples when appropriate.*



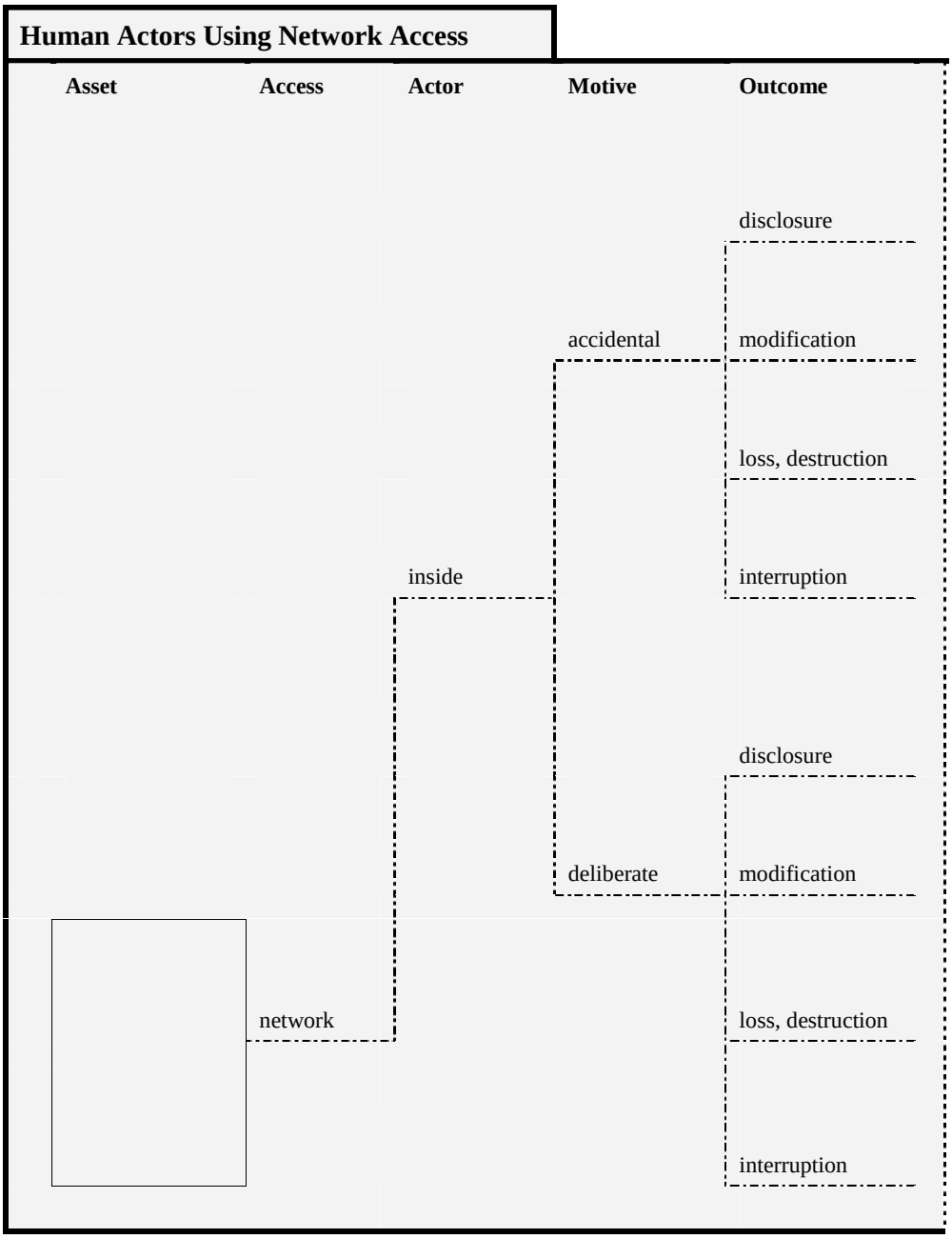
8 Threat Translation Guide

Phase 1
Process S2
Activity S2.3

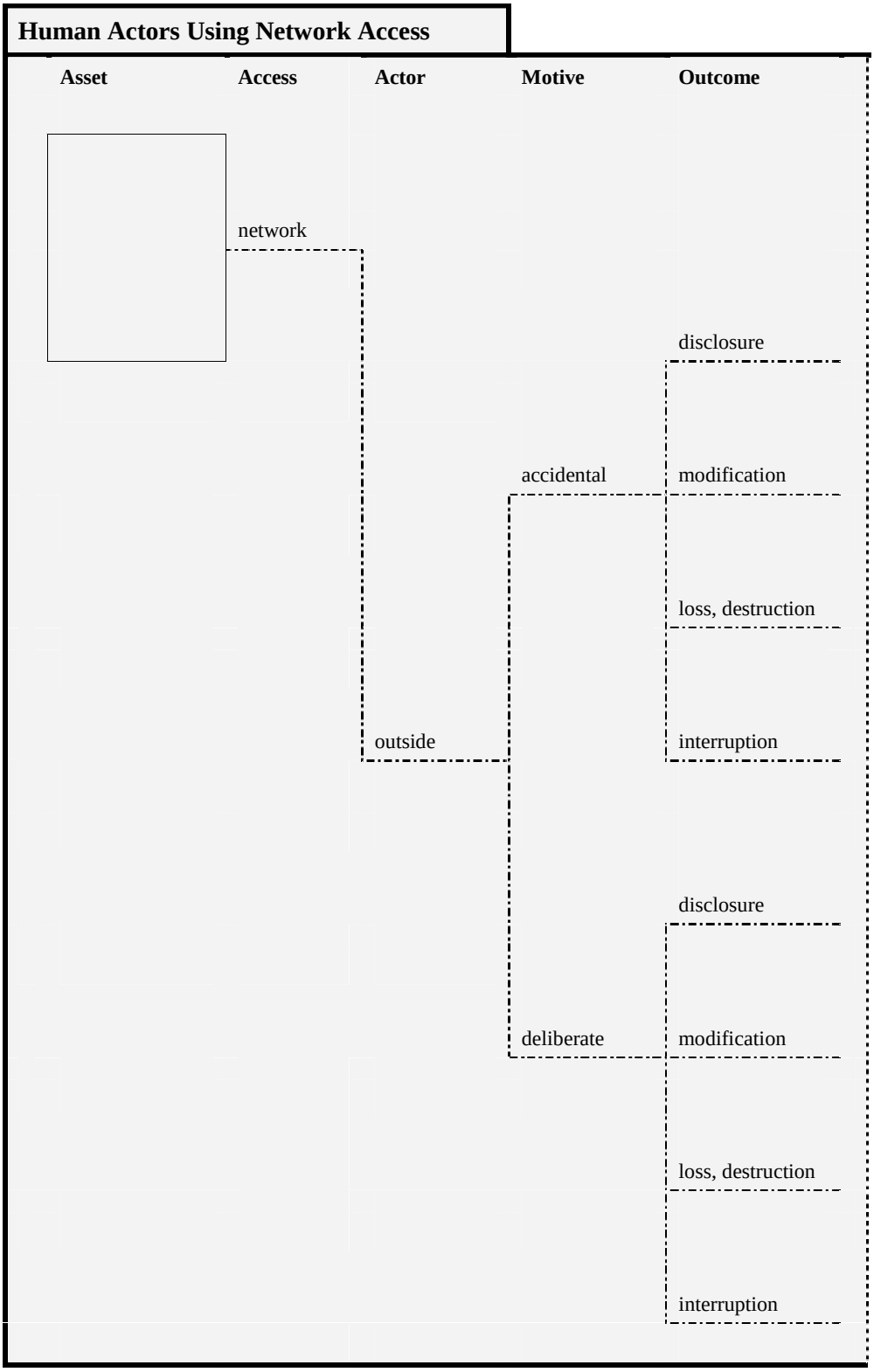
Threat Translation Guide

The *Threat Translation Guide* describes each branch of an asset-based threat tree. If you have difficulty understanding the types of threats represented by a branch, you can use this guide to decipher the meaning of that branch.

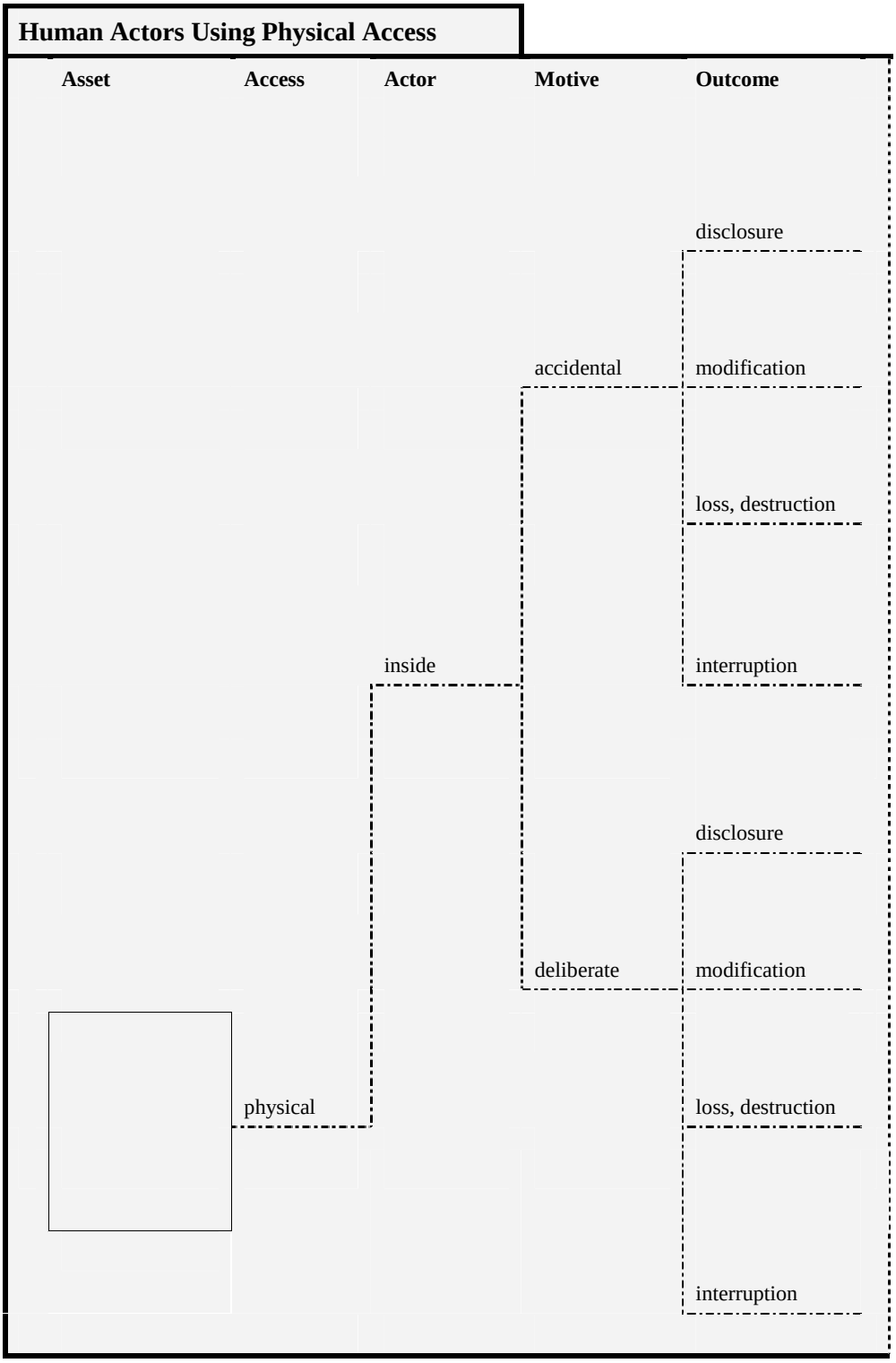
You will find asset-based threat trees for the following sources of threat:


Human Actors Using Network Access
Asset
Access
Actor
Motive
Outcome
disclosure
accidental
modification
loss, destruction
inside
interruption
disclosure
deliberate
modification
network
loss, destruction
interruption

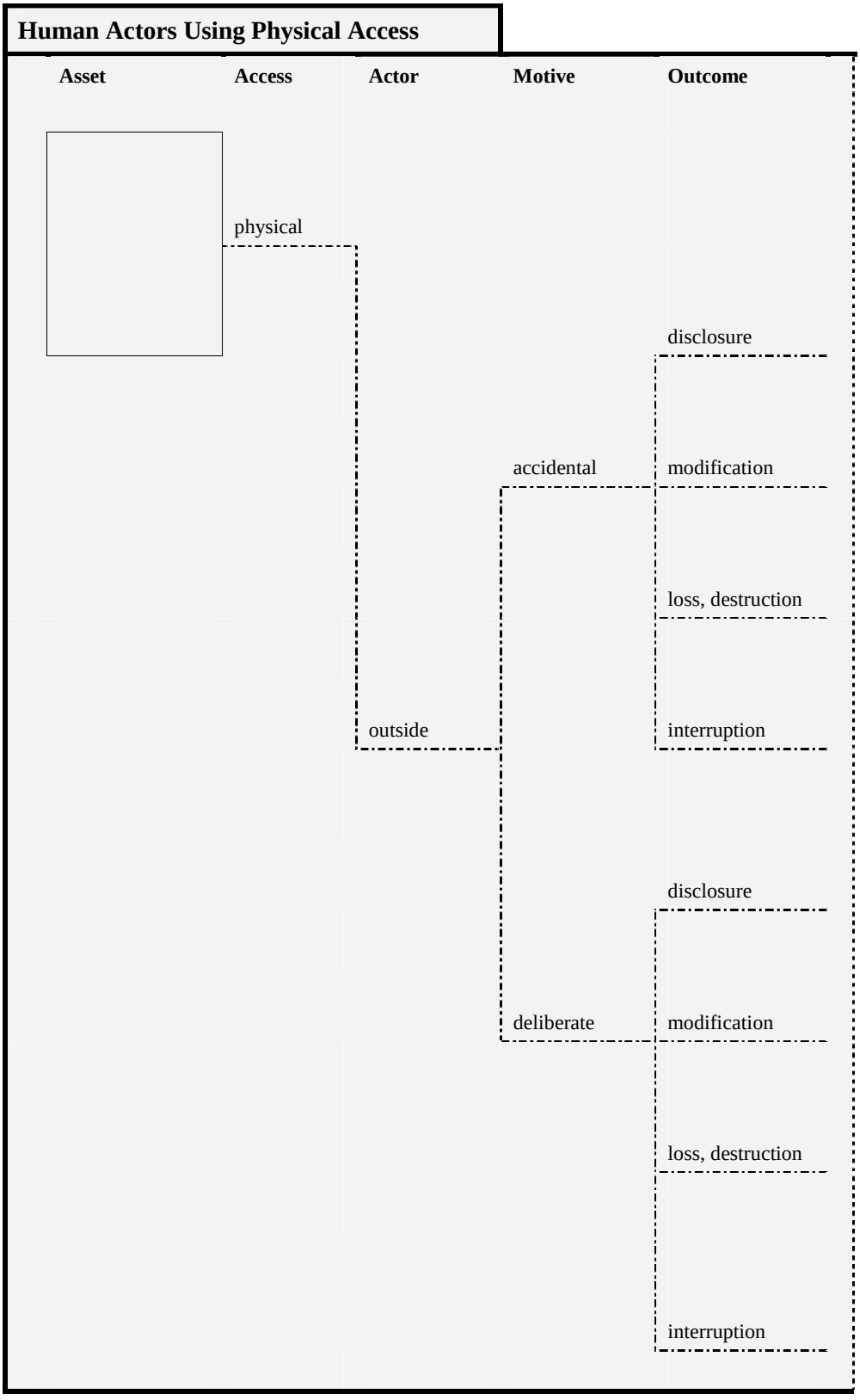
Description	Example
A staff member without malicious intent who has legitimate access to the computing infrastructure accidentally views confidential information on an important system.	Incorrect file permissions enable a staff member to accidentally access a restricted personnel database.
A staff member without malicious intent who has legitimate access to the computing infrastructure accidentally modifies information on an important system.	A staff member accidentally enters incorrect financial data into a customer database.
A staff member without malicious intent who has legitimate access to the computing infrastructure accidentally loses or destroys information on an important system.	A staff member deletes an important customer file by mistake.
A staff member without malicious intent who has legitimate access to the computing infrastructure accidentally interrupts access to an important system.	A staff member who is not computer savvy inadvertently crashes an important system.
A staff member with malicious intent who has legitimate access to the computing infrastructure exploits that access to deliberately view confidential information on an important system.	A staff member uses access to a restricted personnel database to deliberately view information in that database that is restricted by policy.
A staff member with malicious intent who has legitimate access to the computing infrastructure exploits that access to deliberately modify information on an important system.	A staff member responsible for data entry deliberately enters incorrect customer information into a database.
A staff member with malicious intent who has legitimate access to the computing infrastructure exploits that access to deliberately lose or destroy information on an important system.	A staff member with access to design documents for a new product deliberately deletes the files that contain those design documents.
A staff member with malicious intent who has legitimate access to the computing infrastructure exploits that access to deliberately interrupt access to an important system.	A staff member uses legitimate access to the computing infrastructure to launch a denial-of-service attack on an important system.


Human Actors Using Network Access
Asset
Access
Actor
Motive
Outcome
network
outside
accidental
deliberate
disclosure
modification
loss, destruction
interruption
disclosure
modification
loss, destruction
interruption

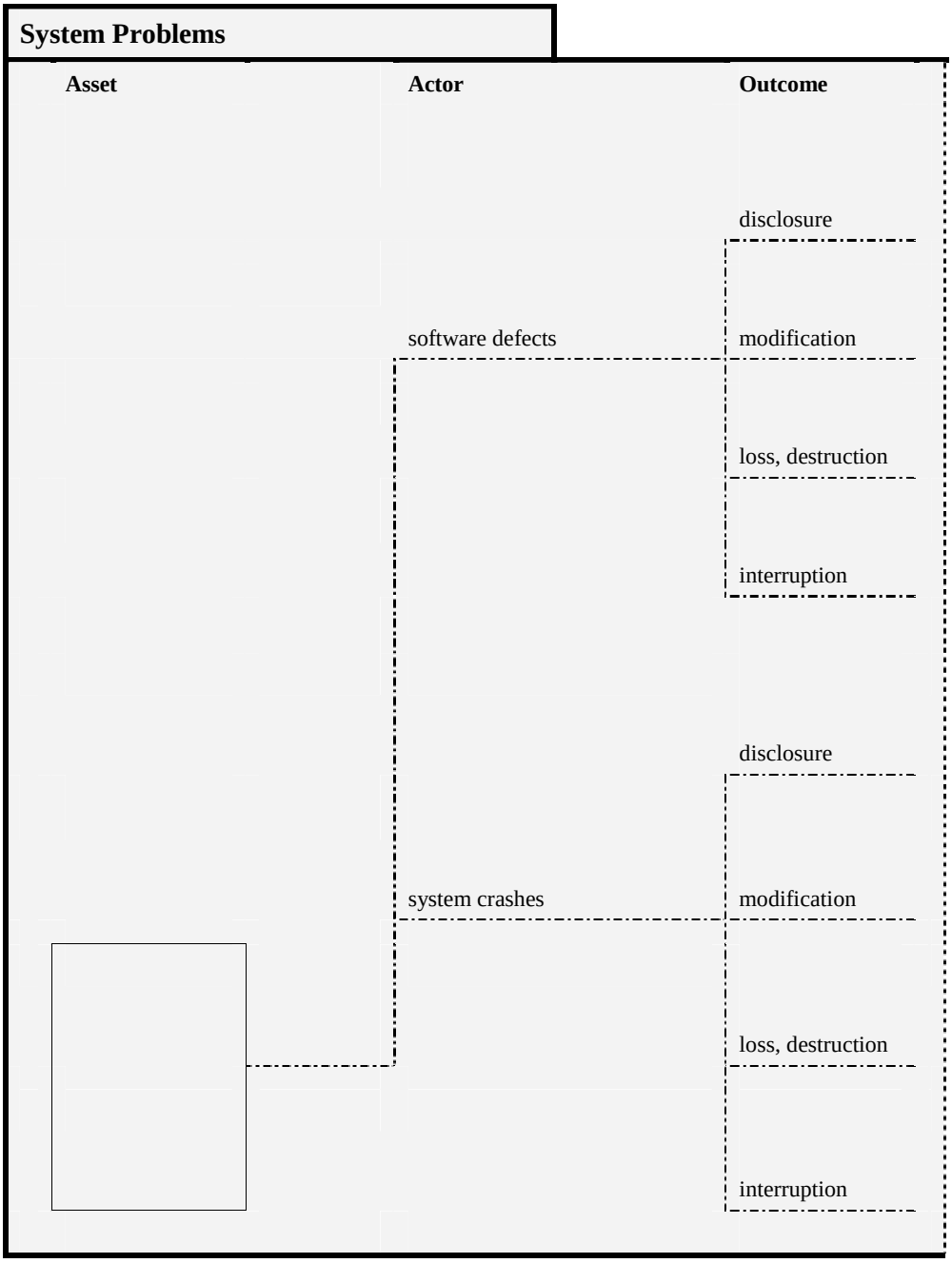
Description	Example
An outsider without malicious intent gains access to your computing infrastructure (legitimately or by accident) and views confidential data on a system.	Temporary employees are given access to your computing infrastructure to help with an increased workload. While performing their job duties, one of them accidentally views confidential personnel data.
An outsider without malicious intent gains access to your computing infrastructure (legitimately or by accident) and accidentally modifies information on a system.	Temporary employees are given access to your computing infrastructure to help with an increased workload. While performing their job duties, one of them accidentally modifies important customer data.
An outsider without malicious intent gains access to your computing infrastructure (legitimately or by accident) and loses or destroys information on a system.	Temporary employees are given access to your computing infrastructure to help with an increased workload. While performing their job duties, one of them accidentally loses or destroys financial data.
An outsider without malicious intent gains access to your computing infrastructure (legitimately or by accident) and accidentally interrupts access to a system.	Temporary employees are given access to your computing infrastructure to help with an increased workload. While performing their job duties, one of them accidentally crashes an important system.
An attacker with malicious intent deliberately exploits vulnerabilities in the computing infrastructure to view confidential information.	A corporate spy exploits vulnerabilities in the computing infrastructure to gain unauthorized access to a key business system. The spy uses that access to view confidential customer information on the system.
An attacker with malicious intent deliberately exploits vulnerabilities in the computing infrastructure to modify information.	A corporate spy exploits vulnerabilities in the computing infrastructure to gain unauthorized access to a key business system. The spy uses that access to modify financial data on the system.
An attacker with malicious intent deliberately exploits vulnerabilities in the computing infrastructure to lose or destroy information.	A corporate spy exploits vulnerabilities in the computing infrastructure to gain unauthorized access to a key business system. The spy uses that access to lose or destroy a new product design on the system.
An attacker with malicious intent deliberately exploits vulnerabilities in the computing infrastructure to interrupt access to a system.	A corporate spy exploits vulnerabilities in the computing infrastructure to gain unauthorized access to an airline's scheduling system. The spy uses that access to crash the system and prevent real-time updates.


Human Actors Using Physical Access
Asset
Access
Actor
Motive
Outcome
disclosure
accidental
modification
loss, destruction
inside
interruption
disclosure
deliberate
modification
physical
loss, destruction
interruption

Description	Example
A staff member without malicious intent accidentally views confidential information after gaining physical access to a system, one of its components, or a physical copy of the information.	A staff member accidentally sees confidential information on (1) a colleague's computer screen or (2) a printout on a colleague's desk.
A staff member without malicious intent accidentally modifies information after gaining physical access to a system, one of its components, or a physical copy of the information.	A staff member modifies information by (1) accidentally altering information on a colleague's computer while using it for another purpose or (2) accidentally taking a page of a printout on a colleague's desk.
A staff member without malicious intent accidentally loses or destroys information after gaining physical access to a system, one of its components, or a physical copy of the information.	A staff member loses or destroys information by (1) accidentally deleting information from a colleague's computer while using it or (2) shredding a paper accidentally taken from a colleague's desk.
A staff member without malicious intent interrupts access to a system or information by accidentally using physical access to a system, one of its components, or a physical copy of the information to prevent others from accessing the system or information.	A staff member interrupts access to a system by (1) accidentally crashing the system while accessing it from a colleague's computer or (2) locking the keys inside an office where a physical file is stored.
A staff member with malicious intent deliberately views confidential information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A staff member uses unauthorized access to a physically restricted area of the building to deliberately (1) view confidential information on a computer or (2) read a confidential memo lying on a desk.
A staff member with malicious intent deliberately modifies information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A staff member uses unauthorized access to a physically restricted area of the building to deliberately (1) modify information on a computer or (2) modify a physical file lying on a desk.
A staff member with malicious intent deliberately loses or destroys information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A staff member uses unauthorized access to a physically restricted area of the building to deliberately (1) delete information on a computer or (2) destroy a physical file lying on a desk.
A staff member with malicious intent deliberately interrupts access to an important system or information by breeching physical security to a system, one of its components, or a physical copy of the information and using that physical access to prevent others from accessing the system or information.	A staff member uses unauthorized access to a physically restricted area of the building to (1) gain access to and then deliberately crash an important business system or (2) jam the door and prevent others from physically accessing the systems and information located in that area of the building.

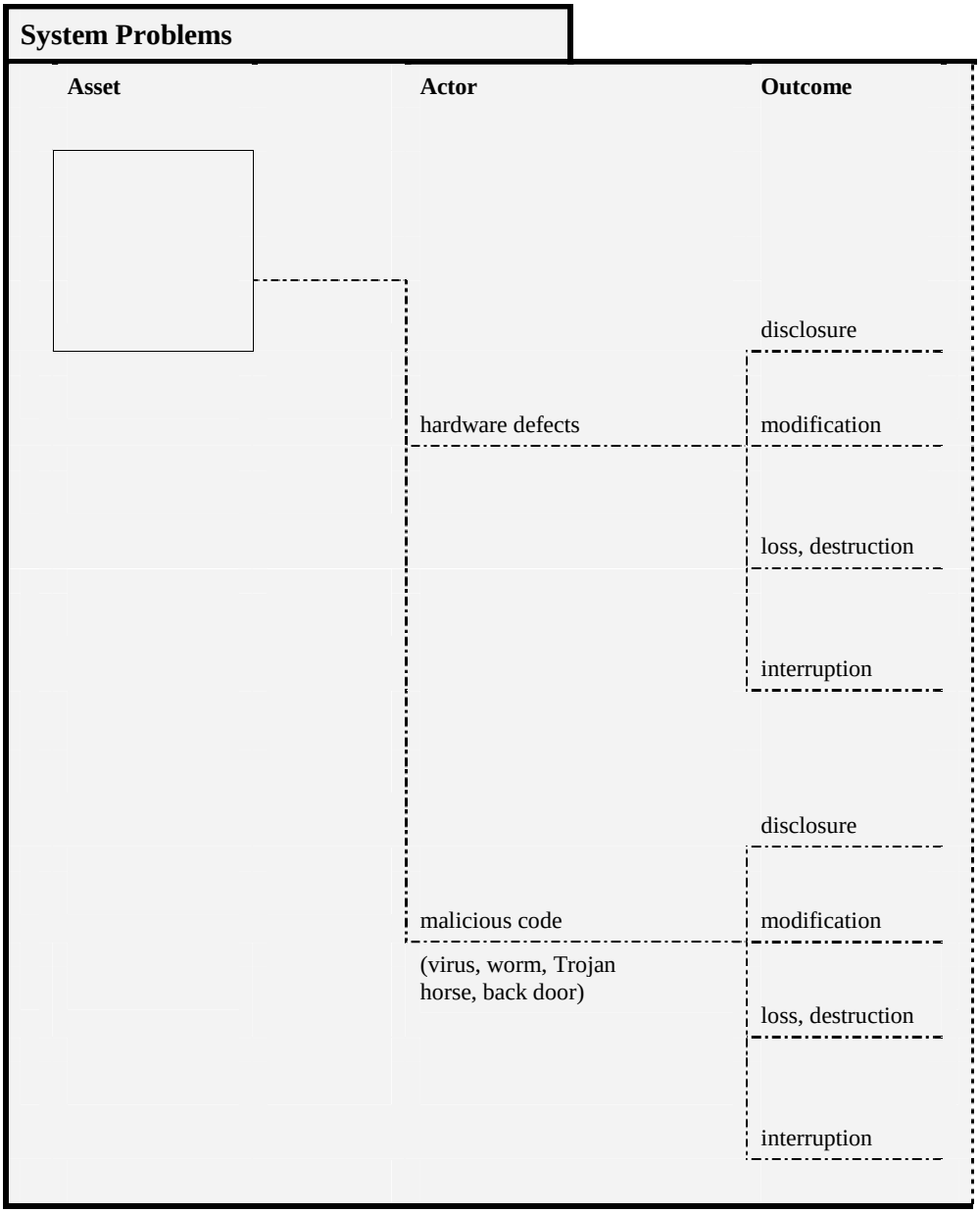

Human Actors Using Physical Access
Asset
Access
Actor
Motive
Outcome
physical
outside
accidental
disclosure
modification
loss, destruction
interruption
deliberate
disclosure
modification
loss, destruction
interruption

Description	Example
An outsider without malicious intent gains physical access to your computing infrastructure or a physical copy of information and uses that access to view confidential information accidentally.	A consultant is given access to a staff member's office and accidentally sees confidential information on (1) a staff member's computer screen or (2) a printout on a staff member's desk.
An outsider without malicious intent gains physical access to your computing infrastructure or a physical copy of information and uses that access to modify information accidentally.	A consultant is given access to the computer room and (1) accidentally makes the wrong change to a configuration file on a server or (2) accidentally records the wrong information in a maintenance log.
An outsider without malicious intent gains physical access to your computing infrastructure or a physical copy of information and uses that access to lose or destroy information accidentally.	A consultant configuring one of your servers is given access to the computer room and accidentally (1) destroys an important electronic file or (2) throws away an important piece of system documentation.
An outsider without malicious intent gains physical access to your computing infrastructure or a physical copy of information and uses that access to accidentally prevent others from accessing the information.	A consultant configuring one of your servers is given access to the computer room and accidentally (1) crashes a system while accessing it or (2) locks the keys to the computer room inside it after he or she leaves.
An attacker with malicious intent deliberately views confidential information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A corporate spy poses as a member of the cleaning crew to gain unauthorized physical access to a competitor's site and view confidential information either (1) on a key business system or (2) in a physical file.
An attacker with malicious intent deliberately modifies information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A corporate spy poses as a member of the cleaning crew to gain unauthorized physical access to a competitor's site and modify financial information either (1) on a key business system or (2) in a physical file.
An attacker with malicious intent deliberately loses or destroys information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A corporate spy poses as a member of the cleaning crew to gain unauthorized physical access to a competitor's site and destroy customer information either (1) on a key business system or (2) in a physical file.
An attacker with malicious intent deliberately interrupts access to an important system or information by breeching physical security to a system, one of its components, or a physical copy of the information and by using that physical access to prevent others from accessing the system or information.	A corporate spy poses as a member of the cleaning crew to gain unauthorized physical access to a competitor's site and (1) deliberately crashes an important business system or (2) jams the door to prevent others from physically accessing the systems and information located in an area of the building.



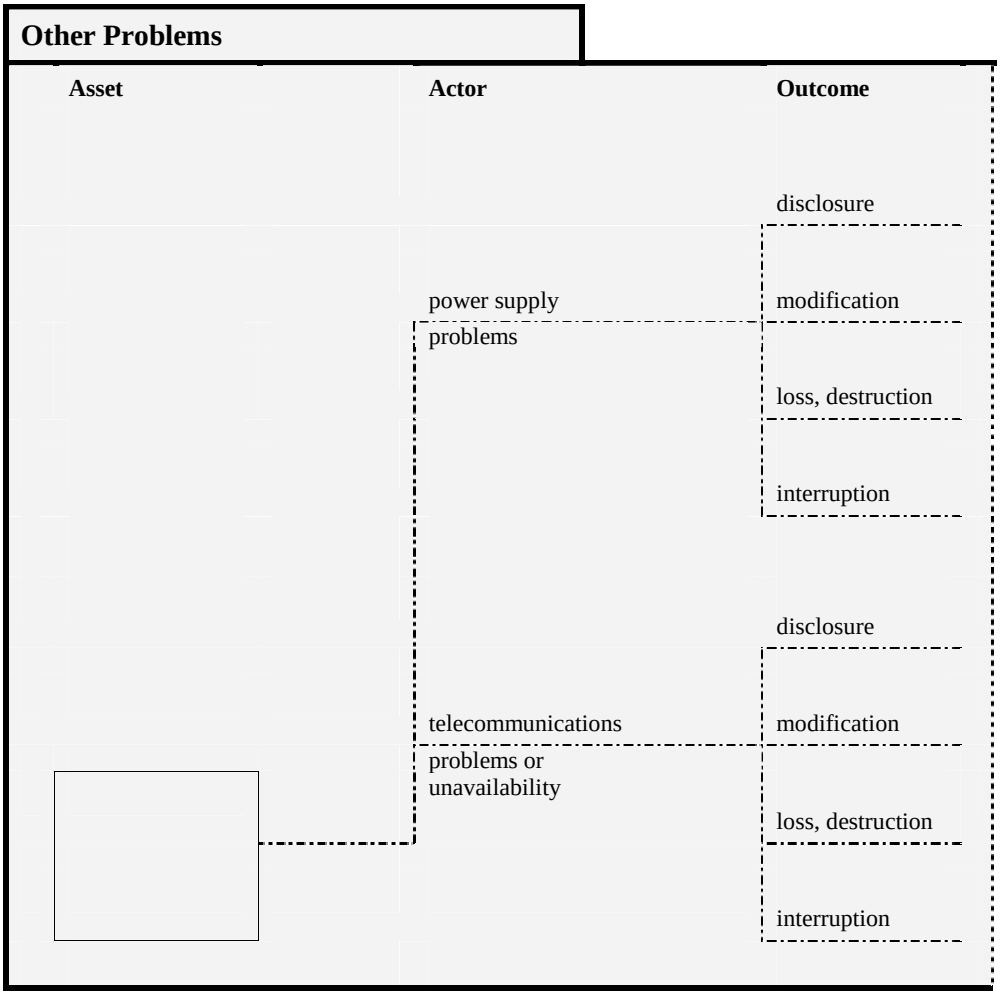
* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
A software defect results in disclosure of information to unauthorized parties.	A defect in a computer's operating system changes file access permissions to permit world read and write permissions on certain files and directories.
A software defect results in modification of information on a system.	A custom software application incorrectly performs mathematical operations on data, affecting the integrity of the results.
A software defect results in the loss or destruction of information on a system.	A word processing application is known to crash computers periodically because of a problem with a specific command sequence, destroying any information that was not saved.
A software defect results in a system crash, preventing access to the system.	A word processing application is known to crash computers periodically because of a problem with a specific command sequence, preventing access to that computer.
A system crashes for unknown reasons (i.e., it cannot be traced to a software defect, hardware defect, malicious code, or actions by people), resulting in disclosure of information to unauthorized parties.	---
A system crashes for unknown reasons (i.e., it cannot be traced to a software defect, hardware defect, malicious code, or actions by people), resulting in modification of information on that system.	A system crashes during a lengthy update of a financial database, corrupting the information in the database.
A system crashes for unknown reasons (i.e., it cannot be traced to a software defect, hardware defect, malicious code, or actions by people), resulting in the loss or destruction of information on that system.	A customer database system frequently crashes, destroying any information that was not saved at the time of the crash.
A system crashes for unknown reasons (i.e., it cannot be traced to a software defect, hardware defect, malicious code, or actions by people), resulting in interruption of access to that system.	An email server crashes, resulting in interruption of user access to email.



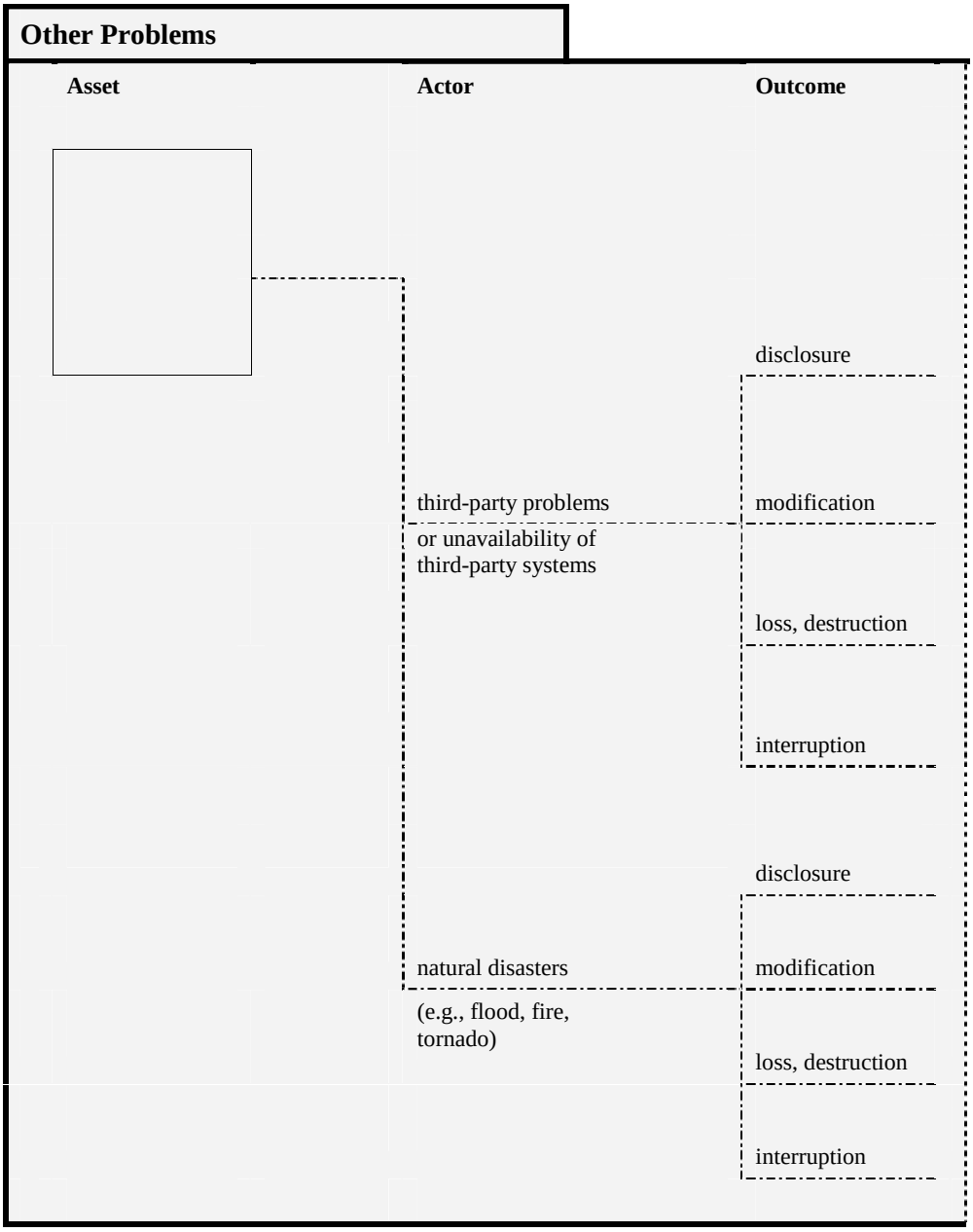
* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
A hardware defect results in disclosure of information to unauthorized parties.	---
A hardware defect results in modification of information on a system.	A disk drive develops a hardware problem that affects the integrity of a database that is stored on the disk.
A hardware defect results in the loss or destruction of information on a system.	A disk drive develops a hardware problem that ends up destroying the information on the disk. Files can be retrieved only from backups.
A hardware defect results in a system crash, preventing access to the system.	A disk drive develops a hardware problem, preventing access to any information on the disk until the problem is corrected.
A system is affected by malicious code (virus, worm, Trojan horse, back door) that enables unauthorized parties to view information.	A back door on a system enables unauthorized people to access the system and view customer credit card information on that system.
A system is affected by malicious code (virus, worm, Trojan horse, back door) that modifies information on that system.	A system is infected with a virus that modifies a process control application on the computer's disk drive.
A system is affected by malicious code (virus, worm, Trojan horse, back door) that deletes information on that system.	A system is infected with a virus that deletes all information on the computer's disk drive.
A system is affected by malicious code (virus, worm, Trojan horse, back door) that results in the system crashing.	A system is infected with a virus that is spread via email, slowing network traffic and creating a denial-of-services attack.



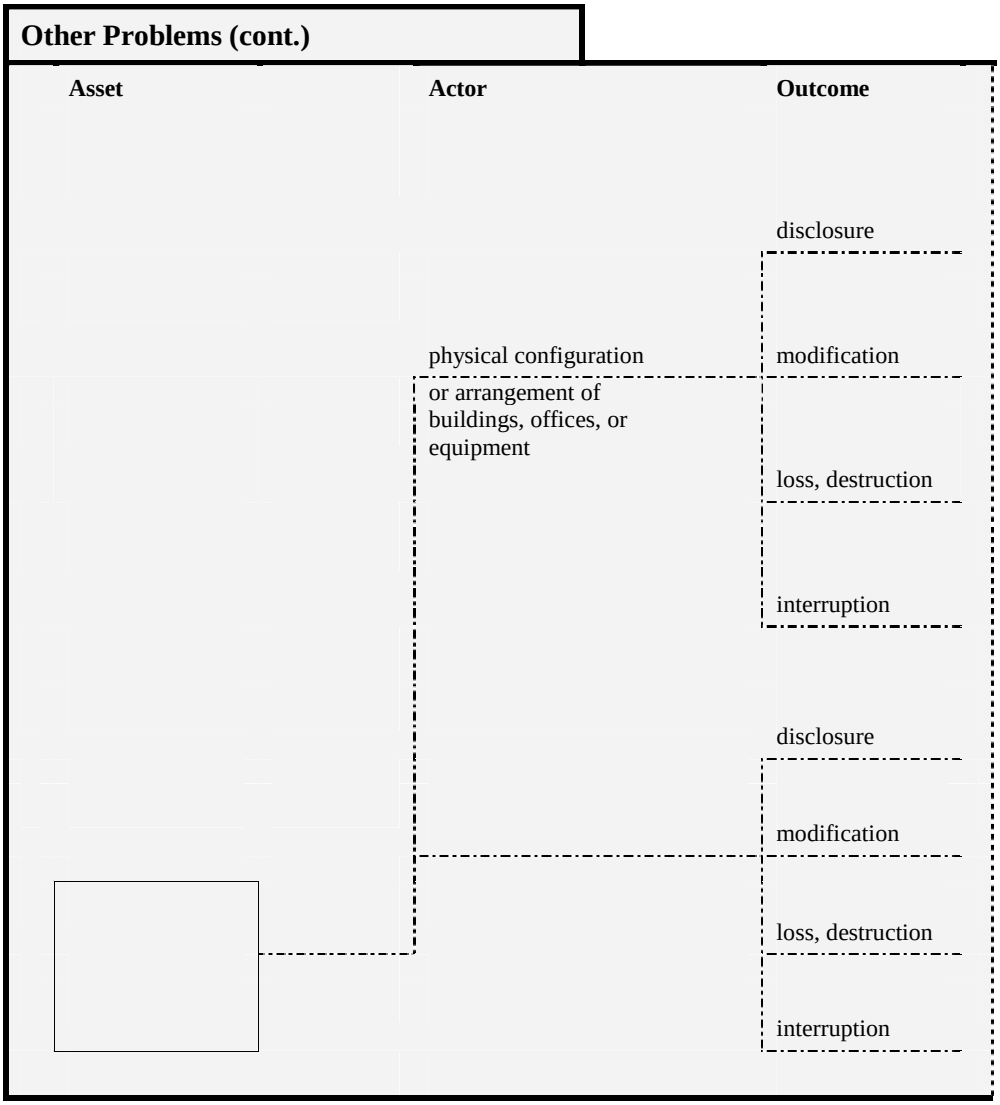
* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
Problems with the power supply lead to disclosure of information to unauthorized parties.	---
Problems with the power supply lead to modification of information on a system.	---
Problems with the power supply lead to loss or destruction of information on a system.	A power outage results in loss of any information that was not saved at the time of the outage.
Problems with the power supply lead to interruption of access to a system.	A power outage prevents access to all key business systems.
Unavailability of telecommunications services leads to disclosure of information to unauthorized parties.	---
Unavailability of telecommunications services leads to modification of information on a system.	---
Unavailability of telecommunications services leads to loss or destruction of information on a system.	---
Unavailability of telecommunications services leads to interruption of access to a system.	The unavailability of the telecommunications link prevents access to a key business system located at a remote site.



* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
Problems with services provided by third parties (e.g., maintenance of systems) lead to disclosure of information to unauthorized parties.	A staff member from a third-party service provider views confidential information on a key business system that is maintained by that service provider.
Problems with services provided by third parties (e.g., maintenance of systems) lead to modification of information on a system.	Problems at a third-party service provider lead to the modification of information on a key business system located at that provider's site and maintained by the provider.
Problems with services provided by third parties (e.g., maintenance of systems) lead to loss or destruction of information on a system.	Problems at a third-party service provider lead to the destruction of information on a key business system located at that provider's site and maintained by the provider.
Problems with services provided by third parties (e.g., maintenance of systems) lead to interruption of access to a system.	A system maintained by a third-party service provider and located at the provider's site is unavailable due to problems created by that provider's staff.
Natural disasters (e.g., flood, fire, tornado) lead to disclosure of information to unauthorized parties.	People at the site of a tornado see confidential memos that are dispersed among the debris.
Natural disasters (e.g., flood, fire, tornado) lead to modification of information.	---
Natural disasters (e.g., flood, fire, tornado) lead to loss or destruction of information.	The flooding of a basement area destroys paper records that are stored there.
Natural disasters (e.g., flood, fire, tornado) lead to interruption of access to a system.	The flooding of a computer room in the basement of a building prevents access to systems in that room.



* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
The physical configuration or arrangement of buildings, offices, or equipment leads to disclosure of information to unauthorized parties.	The layout of an office workspace enables anyone in the area to view customer credit card information displayed on computer screens.
The physical configuration or arrangement of buildings, offices, or equipment leads to modification of information on a system.	---
The physical configuration or arrangement of buildings, offices, or equipment leads to loss or destruction of information on a system.	---
The physical configuration or arrangement of buildings, offices, or equipment leads to interruption of access to a system.	---

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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

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

6. AUTHOR(S)

Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody

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

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

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

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

14. SUBJECT TERMS	15. NUMBER OF PAGES
information security, risk management, OCTAVE	78

16. PRICE CODE

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

OCTAVE®-S Implementation Guide, Version 1.0

Volume 6: Critical Asset Worksheets for Systems

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

HANDBOOK
CMU/SEI-2003-HB-003

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

OCTAVE®-S Implementation Guide, Version 1.0

Volume 6: Critical Asset Worksheets for Systems

CMU/SEI-2003-HB-003

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

Networked Systems Survivability Program

This report was prepared for the

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

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

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

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

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

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

Table of Contents

List of Tables

About This Document

This document is Volume 6 of the *OCTAVE-S Implementation Guide*, a 10-volume handbook supporting the OCTAVE-S methodology. This volume provides worksheets to document data related to critical assets that are categorized as systems.

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℠ (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 Introduction

This document contains the Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE®)-S worksheets related to critical assets that are systems. The activities related to these worksheets are focused on analyzing a critical asset.

Table 1 provides a brief introduction to the contents of this workbook, using activity step numbers as a key. For more details about how to complete each step, refer to the *OCTAVE®-S Method Guidelines*, which can be found in Volume 3 of the *OCTAVE®-S Implementation Guide*.

Table 1: Worksheets Provided in This Workbook

Step	Description	Worksheet	Activity	Pages
Step 6	Start a *Critical Asset Information worksheet* for each critical asset. Record the name of the critical asset on its *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 7	Record your rationale for selecting each critical asset on that asset's *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 8	Record a description for each critical asset on that asset's *Critical Asset Selection worksheet*. Consider who uses each critical asset as well as who is responsible for it.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 9	Record assets that are related to each critical asset on that asset's *Critical Asset Information worksheet*. Refer to the *Asset Identification worksheet* to determine which assets are related to each critical asset.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8

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

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

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 10	Record the security requirements for each critical asset on that asset's *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 11	For each critical asset, record the most important security requirement on that asset's *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 12	Complete all appropriate threat trees for each critical asset. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on any threat tree, review the description and examples of that threat in the *Threat Translation Guide*.	Risk Profile Threat Translation Guide	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-54
Step 13	Record specific examples of threat actors on the *Risk Profile worksheet* for each applicable actor-motive combination.	Risk Profile	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-54
Step 14	Record the strength of the motive for deliberate threats due to human actors. Also record how confident you are in your estimate of the strength of the actor's motive.	Risk Profile	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-54
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.	Risk Profile	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-54
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.	Risk Profile	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-54

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 17	Select the system of interest for each critical asset (i.e., the system most closely related to the critical asset).	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58
Step 18a	Review paths used to access each critical asset, and select key classes of components related to each critical asset. Determine which classes of components are part of the system of interest.	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58
Step 18b	Determine which classes of components serve as intermediate access points (i.e., which components are used to transmit information and applications from the system of interest to people).	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58
Step 18c	Determine which classes of components, both internal and external to the organization's networks, are used by people (e.g., users, attackers) to access the system.	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58
Step 18d	Determine where information from the system of interest is stored for backup purposes.	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58
Step 18e	Determine which other systems access information or applications from the system of interest and which other classes of components can be used to access critical information or services from the system of interest.	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) for each active threat to each critical asset.	Risk Profile Impact Evaluation Criteria	Phase 3 Process S4 S4.1 Evaluate Impacts of Threats	9-54
Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) for each active threat to each critical asset. Document your confidence level in your probability estimate.	Risk Profile Probability Evaluation Criteria	Phase 3 Process S4 S4.3 Evaluate Probabilities of Threats	9-54
Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of each critical asset's *Risk Profile worksheet*.	Risk Profile Security Practices	Phase 3 Process S5 S5.2 Select Mitigation Approaches	9-54
Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.	Risk Profile	Phase 3 Process S5 S5.2 Select Mitigation Approaches	9-54

2 Critical Asset Information Worksheet for Systems

Phase 1
Process S2
Activity S2.1

Step 6	Start a *Critical Asset Information worksheet* for each critical asset. Record the name of the critical asset on its *Critical Asset Information worksheet*.
Step 7	Record your rationale for selecting each critical asset on that asset's *Critical Asset Information worksheet*.
Step 8	Record a description for each critical asset on that asset's *Critical Asset Selection worksheet*. Consider who uses each critical asset as well as who is responsible for it.
Step 9	Record assets that are related to each critical asset on that asset's *Critical Asset Information worksheet*. Refer to the *Asset Identification worksheet* to determine which assets are related to each critical asset.

Phase 1
Process S2
Activity S2.2

Step 10	Record the security requirements for each critical asset on that asset's *Critical Asset Information worksheet*.
Step 11	For each critical asset, record the most important security requirement on that asset's *Critical Asset Information worksheet*.

Step 6 **Step 7**

Critical Asset	**Rationale for Selection**
What is the critical system?	*Why is this system critical to the organization?*

Step 9

Related Assets	
Which assets are related to this system?	
Information:	Applications:
Other:	

Step 8

Description	
Who uses the system?	*Who is responsible for the system?*

Step 10

Security Requirements		**Step 11** **Most Important Security Requirement**
What are the security requirements for this system? *(Hint: Focus on what the security requirements should be for this system, not what they currently are.)*		*Which security requirement is most important for this system?*
❑ Confidentiality	Only authorized personnel can view information on _____.	❑ Confidentiality
❑ Integrity	Only authorized personnel can modify information on _____.	❑ Integrity ❑ Availability
❑ Availability	_____ must be available for personnel to perform their jobs. Unavailability cannot exceed _____ hour(s) per every _____ hours.	❑ Other
❑ Other	_____ _____	

3 Risk Profile Worksheet for Systems - Human Actors Using Network Access

Phase 1
Process S2
Activity S2.3

Step 12	Complete the threat tree for *human actors using network access*. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on the threat tree, review the description and examples of that threat in the *Threat Translation Guide* (see pp. 60-63 of this workbook).
Step 13	Record specific examples of threat actors on the *Risk Profile worksheet* for each applicable actor-motive combination.
Step 14	Record the strength of the motive for deliberate threats due to human actors. Also record how confident you are in your estimate of the strength of the actor's motive.
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.

continued

	Phase 3 Process S4 Activity S4.1
Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) to each active threat.

	Phase 3 Process S4 Activity S4.3
Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) to each active threat. Document your confidence level in your probability estimate.

	Phase 3 Process S5 Activity S5.2
Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of the following worksheet.

Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.

Human Actors Using Network Access **Basic Risk Profile**

Step 12

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Step 22

Impact Values

What is the potential impact on the organization in each applicable area?

Asset	Access	Actor	Motive	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other
	network	inside	accidental	disclosure						
				modification						
				loss, destruction						
				interruption						
			deliberate	disclosure						
				modification						
				loss, destruction						
				interruption						
		outside	accidental	disclosure						
				modification						
				loss, destruction						
				interruption						
			deliberate	disclosure						
				modification						
				loss, destruction						
				interruption						

Basic Risk Profile | **Human Actors Using Network Access**

Step 24

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Step 26

Security Practice Areas

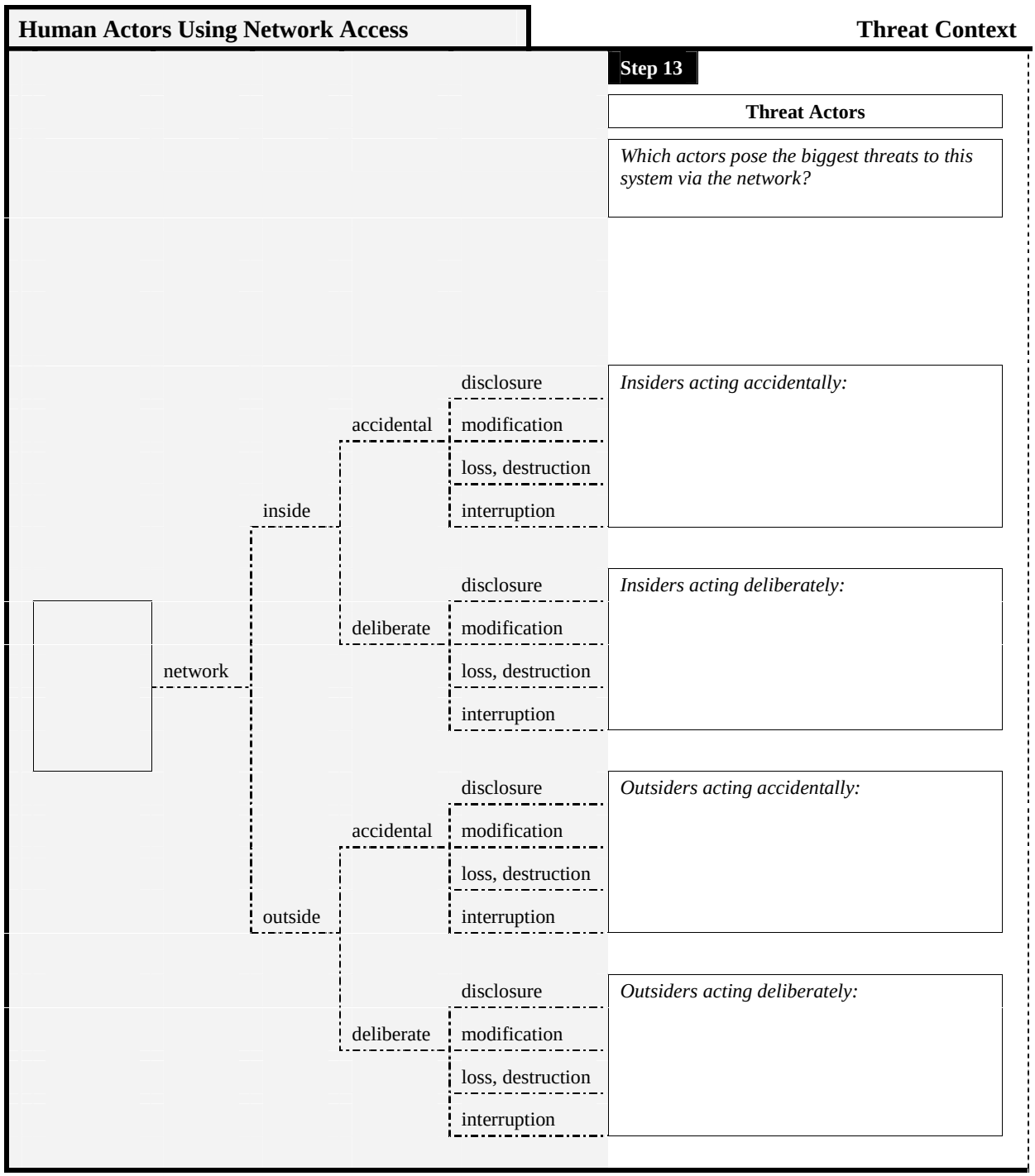
What is the stoplight status for each security practice area?

Step 27

Approach

What is your approach for addressing each risk?

Value	Confidence			Strategic						Operational									Approach		
	Very	Somewhat	Not At All	1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt	Accept	Defer	Mitigate
		|--------|--------|																	❑	❑	❑
		|--------|--------|																	❑	❑	❑
		|--------|--------|																	❑	❑	❑
		|--------|--------|																	❑	❑	❑
		|--------|--------|																	❑	❑	❑
		|--------|--------|																	❑	❑	❑
		|--------|--------|																	❑	❑	❑
		|--------|--------|																	❑	❑	❑
		|--------|--------|																	❑	❑	❑
		|--------|--------|																	❑	❑	❑
		|--------|--------|																	❑	❑	❑
		|--------|--------|																	❑	❑	❑
		|--------|--------|																	❑	❑	❑
		|--------|--------|																	❑	❑	❑
		|--------|--------|																	❑	❑	❑
		|--------|--------|																	❑	❑	❑
		|--------|--------|																	❑	❑	❑


Human Actors Using Network Access
Threat Context
Step 13
Threat Actors
Which actors pose the biggest threats to this system via the network?
network
inside
outside
accidental
deliberate
disclosure
modification
loss, destruction
interruption
Insiders acting accidentally:
Insiders acting deliberately:
Outsiders acting accidentally:
Outsiders acting deliberately:

Threat Context | **Human Actors Using Network Access**

Step 14 | **Step 15**

Motive						History			
How strong is the actor's motive?			*How confident are you in this estimate?*			*How often has this threat occurred in the past?*	*How accurate are the data?*		
High	**Medium**	**Low**	**Very**	**Somewhat**	**Not At All**		**Very**	**Somewhat**	**Not At All**
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑

Step 16

Human Actors Using Network Access	Areas of Concern

Insiders Using Network Access

Give examples of how *insiders acting accidentally* could use network access to threaten this system.	
Give examples of how *insiders acting deliberately* could use network access to threaten this system.	

Outsiders Using Network Access

Give examples of how *outsiders acting accidentally* could use network access to threaten this system.	
Give examples of how *outsiders acting deliberately* could use network access to threaten this system.	

Areas of Concern

Insiders Using Network Access

Outsiders Using Network Access

4 Risk Profile Worksheet for Systems - Human Actors Using Physical Access

Phase 1
Process S2
Activity S2.3

Step 12	Complete the threat tree for *human actors using physical access*. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on the threat tree, review the description and examples of that threat in the *Threat Translation Guide* (see pp. 64-67 of this workbook).
Step 13	Record specific examples of threat actors on the *Risk Profile worksheet* for each applicable actor-motive combination.
Step 14	Record the strength of the motive for deliberate threats due to human actors. Also record how confident you are in your estimate of the strength of the actor's motive.
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.

continued

	Phase 3 Process S4 Activity S4.1
Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) to each active threat.

	Phase 3 Process S4 Activity S4.3
Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) to each active threat. Document your confidence level in your probability estimate.

	Phase 3 Process S5 Activity S5.2
Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of the following worksheet.

Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.

Human Actors Using Physical Access | **Basic Risk Profile**

Step 12

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Step 22

Impact Values

What is the potential impact on the organization in each applicable area?

Asset	Access	Actor	Motive	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other
	physical	inside	accidental	disclosure						
				modification						
				loss, destruction						
				interruption						
			deliberate	disclosure						
				modification						
				loss, destruction						
				interruption						
		outside	accidental	disclosure						
				modification						
				loss, destruction						
				interruption						
			deliberate	disclosure						
				modification						
				loss, destruction						
				interruption						

Basic Risk Profile | **Human Actors Using Physical Access**

Step 24 | **Step 26** | **Step 27**

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value **Confidence**

	Very	Somewhat	Not At All
☐	|--------|--------|		

Security Practice Areas

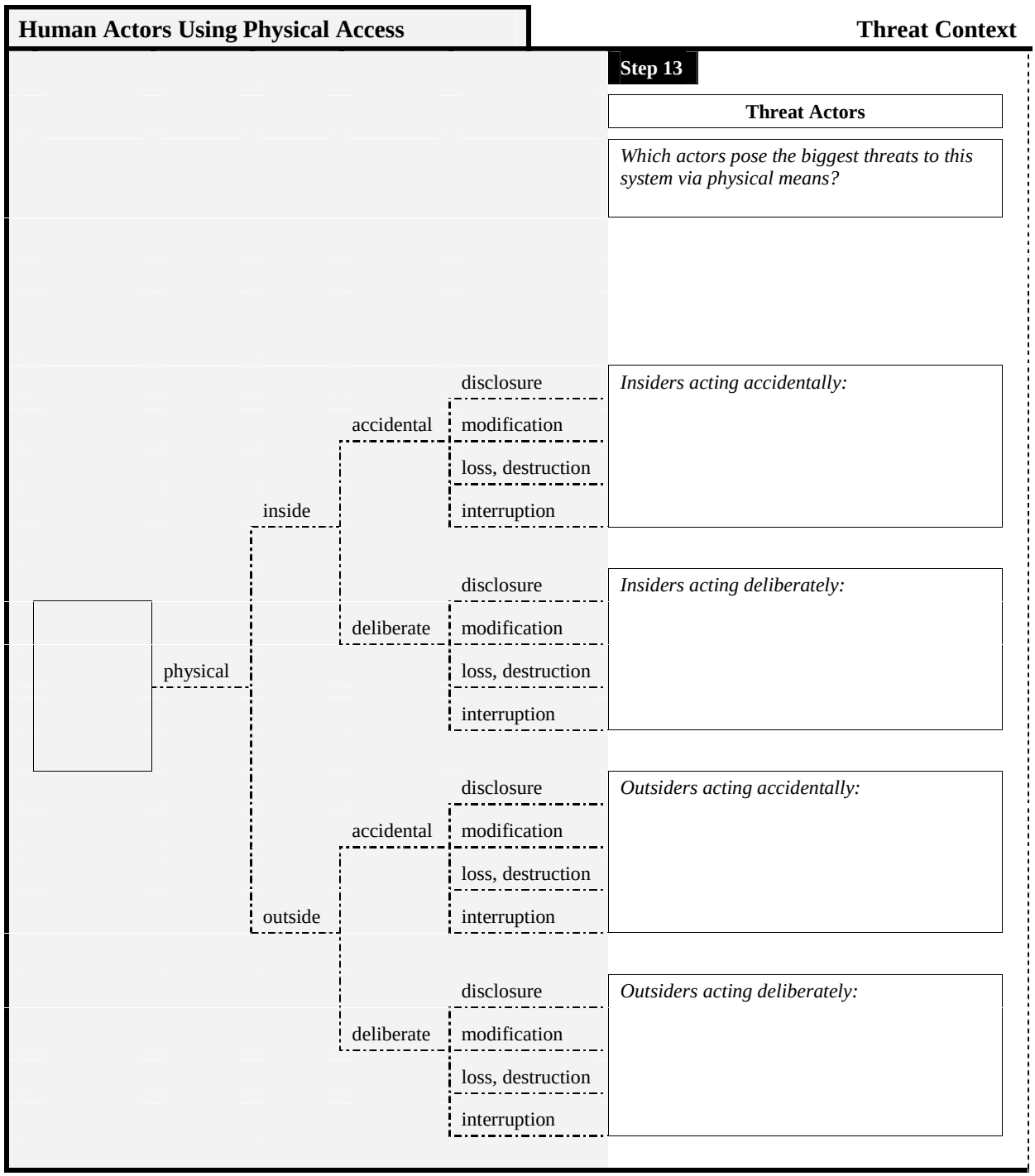
What is the stoplight status for each security practice area?

	Strategic						Operational								
	1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt
☐															
☐															
☐															
☐															
☐															
☐															
☐															
☐															
☐															
☐															
☐															
☐															
☐															
☐															
☐															

Approach

What is your approach for addressing each risk?

	Accept	Defer	Mitigate
☐	☐	☐	☐


Human Actors Using Physical Access
Threat Context
Step 13
Threat Actors
Which actors pose the biggest threats to this system via physical means?
physical
inside
outside
accidental
deliberate
disclosure
modification
loss, destruction
interruption
Insiders acting accidentally:
Insiders acting deliberately:
Outsiders acting accidentally:
Outsiders acting deliberately:

Threat Context | **Human Actors Using Physical Access**

Step 14 | **Step 15**

Motive						History			
How strong is the actor's motive?			*How confident are you in this estimate?*			*How often has this threat occurred in the past?*	*How accurate are the data?*		
High	**Medium**	**Low**	**Very**	**Somewhat**	**Not At All**		**Very**	**Somewhat**	**Not At All**
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑

Step 16

Human Actors Using Physical Access	Areas of Concern

Insiders Using Physical Access

Give examples of how *insiders acting accidentally* could use physical access to threaten this system.	
Give examples of how *insiders acting deliberately* could use physical access to threaten this system.	

Outsiders Using Physical Access

Give examples of how *outsiders acting accidentally* could use physical access to threaten this system.	
Give examples of how *outsiders acting deliberately* could use physical access to threaten this system.	

Areas of Concern

Insiders Using Physical Access

Outsiders Using Physical Access

5 Risk Profile Worksheet for Systems - System Problems

Phase 1
Process S2
Activity S2.3

Step 12	Complete the threat tree for *system problems*. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on the threat tree, review the description and examples of that threat in the *Threat Translation Guide* (see pp. 68-71 of this workbook).
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.

continued

	Phase 3 **Process S4** **Activity S4.1**
Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) to each active threat.

	Phase 3 **Process S4** **Activity S4.3**
Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) to each active threat. Document your confidence level in your probability estimate.

	Phase 3 **Process S5** **Activity S5.2**
Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of the following worksheet.

Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.

System Problems | **Basic Risk Profile**

Step 12 | **Step 22**

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Impact Values

What is the potential impact on the organization in each applicable area?

Asset	Actor	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other
	software defects	disclosure						
		modification						
		loss, destruction						
		interruption						
	system crashes	disclosure						
		modification						
		loss, destruction						
		interruption						
	hardware defects	disclosure						
		modification						
		loss, destruction						
		interruption						
	malicious code (virus, worm, Trojan horse, back door)	disclosure						
		modification						
		loss, destruction						
		interruption						

Basic Risk Profile | **System Problems**

Step 24 | **Step 26** | **Step 27**

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

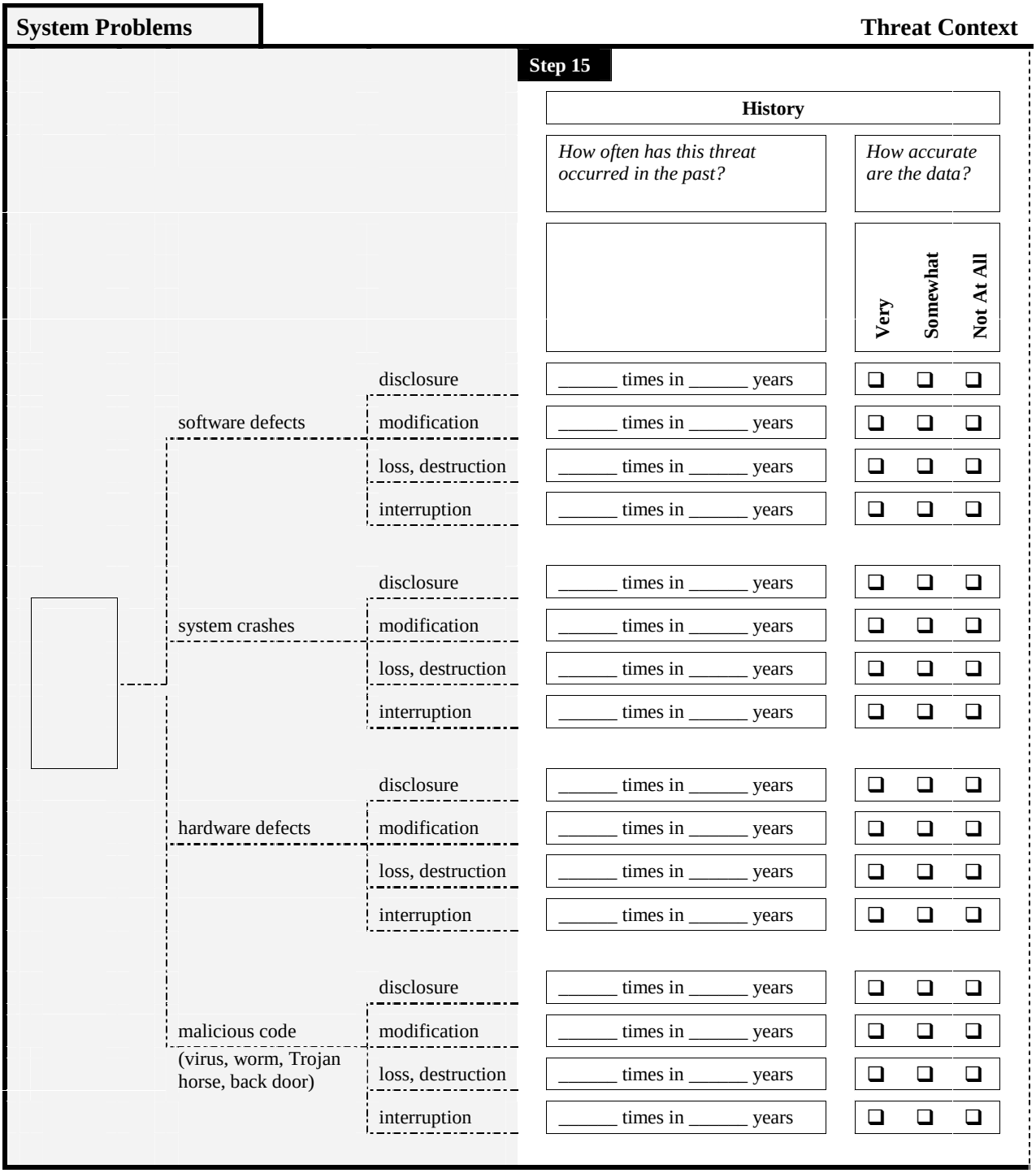
Security Practice Areas

What is the stoplight status for each security practice area?

Approach

What is your approach for addressing each risk?

Value	Confidence			Strategic						Operational									Approach		
	Very	Somewhat	Not At All	1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt	Accept	Defer	Mitigate
	|--------|																		❑	❑	❑
	|--------|																		❑	❑	❑
	|--------|																		❑	❑	❑
	|--------|																		❑	❑	❑
	|--------|																		❑	❑	❑
	|--------|																		❑	❑	❑
	|--------|																		❑	❑	❑
	|--------|																		❑	❑	❑
	|--------|																		❑	❑	❑
	|--------|																		❑	❑	❑
	|--------|																		❑	❑	❑
	|--------|																		❑	❑	❑
	|--------|																		❑	❑	❑
	|--------|																		❑	❑	❑
	|--------|																		❑	❑	❑
	|--------|																		❑	❑	❑


System Problems
Threat Context
Step 15
History
How often has this threat occurred in the past?
How accurate are the data?
Very
Somewhat
Not At All
software defects
system crashes
hardware defects
malicious code
(virus, worm, Trojan horse, back door)
disclosure
modification
loss, destruction
interruption
_____ times in _____ years

Threat Context	System Problems

Notes
What additional notes about each threat do you want to record?

Step 16

System Problems	Areas of Concern
Software Defects	
Give examples of how *software defects* could threaten this system.	
System Crashes	
Give examples of how *system crashes* could threaten this system.	
Hardware Defects	
Give examples of how *hardware defects* could threaten this system.	
Malicious Code	
Give examples of how *malicious code* could threaten this system. (Consider viruses, worms, Trojan horses, back doors, others)	

Areas of Concern

Software Defects
System Crashes
Hardware Defects
Malicious Code

6 Risk Profile Worksheet for Systems - Other Problems

Phase 1
Process S2
Activity S2.3

Step 12	Complete the threat tree for *other problems*. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on the threat tree, review the description and examples of that threat in the *Threat Translation Guide* (see pp. 72-77 of this workbook).
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.

continued

	Phase 3 Process S4 Activity S4.1
Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) to each active threat.

	Phase 3 Process S4 Activity S4.3
Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) to each active threat. Document your confidence level in your probability estimate.

	Phase 3 Process S5 Activity S5.2
Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of the following worksheet.

Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.

Other Problems | **Basic Risk Profile**

Step 12

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Step 22

Impact Values

What is the potential impact on the organization in each applicable area?

Asset	Actor	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other
	power supply problems	disclosure						
		modification						
		loss, destruction						
		interruption						
	telecommunications problems or unavailability	disclosure						
		modification						
		loss, destruction						
		interruption						
	third-party problems or unavailability of third-party systems	disclosure						
		modification						
		loss, destruction						
		interruption						
	natural disasters (e.g., flood, fire, tornado)	disclosure						
		modification						
		loss, destruction						
		interruption						

Basic Risk Profile | **Other Problems**

Step 24 | **Step 26** | **Step 27**

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Security Practice Areas

What is the stoplight status for each security practice area?

Approach

What is your approach for addressing each risk?

Value	Confidence			Strategic						Operational									Approach		
	Very	Somewhat	Not At All	1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt	Accept	Defer	Mitigate
	|--------|--------|																	❑	❑	❑
	|--------|--------|																	❑	❑	❑
	|--------|--------|																	❑	❑	❑
	|--------|--------|																	❑	❑	❑
	|--------|--------|																	❑	❑	❑
	|--------|--------|																	❑	❑	❑
	|--------|--------|																	❑	❑	❑
	|--------|--------|																	❑	❑	❑
	|--------|--------|																	❑	❑	❑
	|--------|--------|																	❑	❑	❑
	|--------|--------|																	❑	❑	❑
	|--------|--------|																	❑	❑	❑
	|--------|--------|																	❑	❑	❑
	|--------|--------|																	❑	❑	❑
	|--------|--------|																	❑	❑	❑
	|--------|--------|																	❑	❑	❑

Other Problems

Threat Context

Step 15

			History			
			How often has this threat occurred in the past?	*How accurate are the data?*		
				Very	**Somewhat**	**Not At All**
		disclosure	_____ times in _____ years	❑	❑	❑
	power supply	modification	_____ times in _____ years	❑	❑	❑
	problems	loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑
		disclosure	_____ times in _____ years	❑	❑	❑
	telecommunications	modification	_____ times in _____ years	❑	❑	❑
	problems or unavailability	loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑
		disclosure	_____ times in _____ years	❑	❑	❑
	third-party problems	modification	_____ times in _____ years	❑	❑	❑
	or unavailability of third-party systems	loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑
		disclosure	_____ times in _____ years	❑	❑	❑
	natural disasters	modification	_____ times in _____ years	❑	❑	❑
	(e.g., flood, fire, tornado)	loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑

Threat Context | **Other Problems**

Notes
What additional notes about each threat do you want to record?

Step 16

Other Problems	Areas of Concern
Power Supply Problems	
Give examples of how *power supply problems* could threaten this system.	
Telecommunications Problems	
Give examples of how *telecommunications problems* could threaten this system.	
Third-Party Problems	
Give examples of how *third-party problems* could threaten this system.	
Natural Disasters	
Give examples of how *natural disasters* could threaten this system.	

Areas of Concern

Power Supply Problems
Telecommunications Problems
Third-Party Problems
Natural Disasters

Other Problems (cont.) **Basic Risk Profile**

Step 12

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Step 22

Impact Values

What is the potential impact on the organization in each applicable area?

Asset	Actor	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other
	physical configuration or arrangement of buildings, offices, or equipment	disclosure						
		modification						
		loss, destruction						
		interruption						
		disclosure						
		modification						
		loss, destruction						
		interruption						
		disclosure						
		modification						
		loss, destruction						
		interruption						
		disclosure						
		modification						
		loss, destruction						
		interruption						

Basic Risk Profile | **Other Problems (cont.)**

Step 24

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value	Confidence	
	Very	
	Somewhat	
	Not At All	

Step 26

Security Practice Areas

What is the stoplight status for each security practice area?

Strategic						Operational									
1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt

Step 27

Approach

What is your approach for addressing each risk?

Accept	Defer	Mitigate
❑	❑	❑

Other Problems (cont.)

Threat Context

Step 15

		History			
		How often has this threat occurred in the past?	*How accurate are the data?*		
			Very	**Somewhat**	**Not At All**
physical configuration or arrangement of buildings, offices, or equipment	disclosure	_____ times in _____ years	❑	❑	❑
	modification	_____ times in _____ years	❑	❑	❑
	loss, destruction	_____ times in _____ years	❑	❑	❑
	interruption	_____ times in _____ years	❑	❑	❑
	disclosure	_____ times in _____ years	❑	❑	❑
	modification	_____ times in _____ years	❑	❑	❑
	loss, destruction	_____ times in _____ years	❑	❑	❑
	interruption	_____ times in _____ years	❑	❑	❑
	disclosure	_____ times in _____ years	❑	❑	❑
	modification	_____ times in _____ years	❑	❑	❑
	loss, destruction	_____ times in _____ years	❑	❑	❑
	interruption	_____ times in _____ years	❑	❑	❑
	disclosure	_____ times in _____ years	❑	❑	❑
	modification	_____ times in _____ years	❑	❑	❑
	loss, destruction	_____ times in _____ years	❑	❑	❑
	interruption	_____ times in _____ years	❑	❑	❑

Threat Context | **Other Problems (cont.)**

Notes
What additional notes about each threat do you want to record?

Step 16

Other Problems (cont.)	**Areas of Concern**
Physical Configuration Problems	
Give examples of how *physical configuration of buildings, offices, or equipment* could threaten this system.	
Give examples of how _____ could threaten this system.	
Give examples of how _____ could threaten this system.	
Give examples of how _____ could threaten this system.	

Areas of Concern

	Physical Configuration Problems

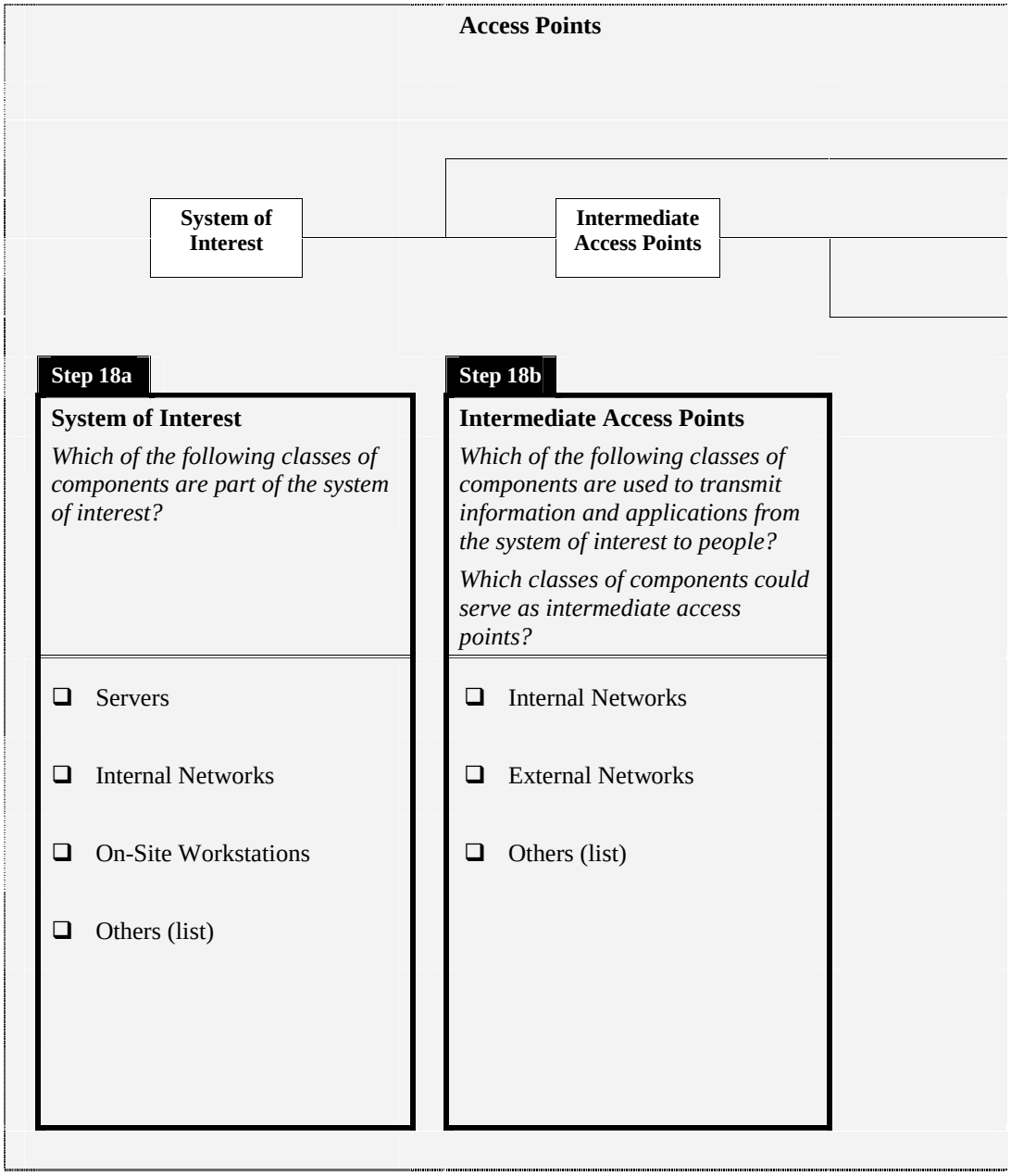
7 Network Access Paths Worksheet

Phase 2 Process S3 Activity S3.1	
Step 17	Select the system of interest for each critical asset (i.e., the system most closely related to the critical asset).
Step 18a	Review paths used to access each critical asset, and select key classes of components related to each critical asset. Determine which classes of components are part of the system of interest.
Step 18b	Determine which classes of components serve as intermediate access points (i.e., which components are used to transmit information and applications from the system of interest to people).
Step 18c	Determine which classes of components, both internal and external to the organization's networks, are used by people (e.g., users, attackers) to access the system.
Step 18d	Determine where information from the system of interest is stored for backup purposes.
Step 18e	Determine which other systems access information or applications from the system of interest and which other classes of components can be used to access critical information or services from the system of interest.

Step 17

System of Interest

What system or systems are most closely related to the critical asset?



Step 18a

System of Interest

Which of the following classes of components are part of the system of interest?

- ❑ Servers
- ❑ Internal Networks
- ❑ On-Site Workstations
- ❑ Others (list)

Step 18b

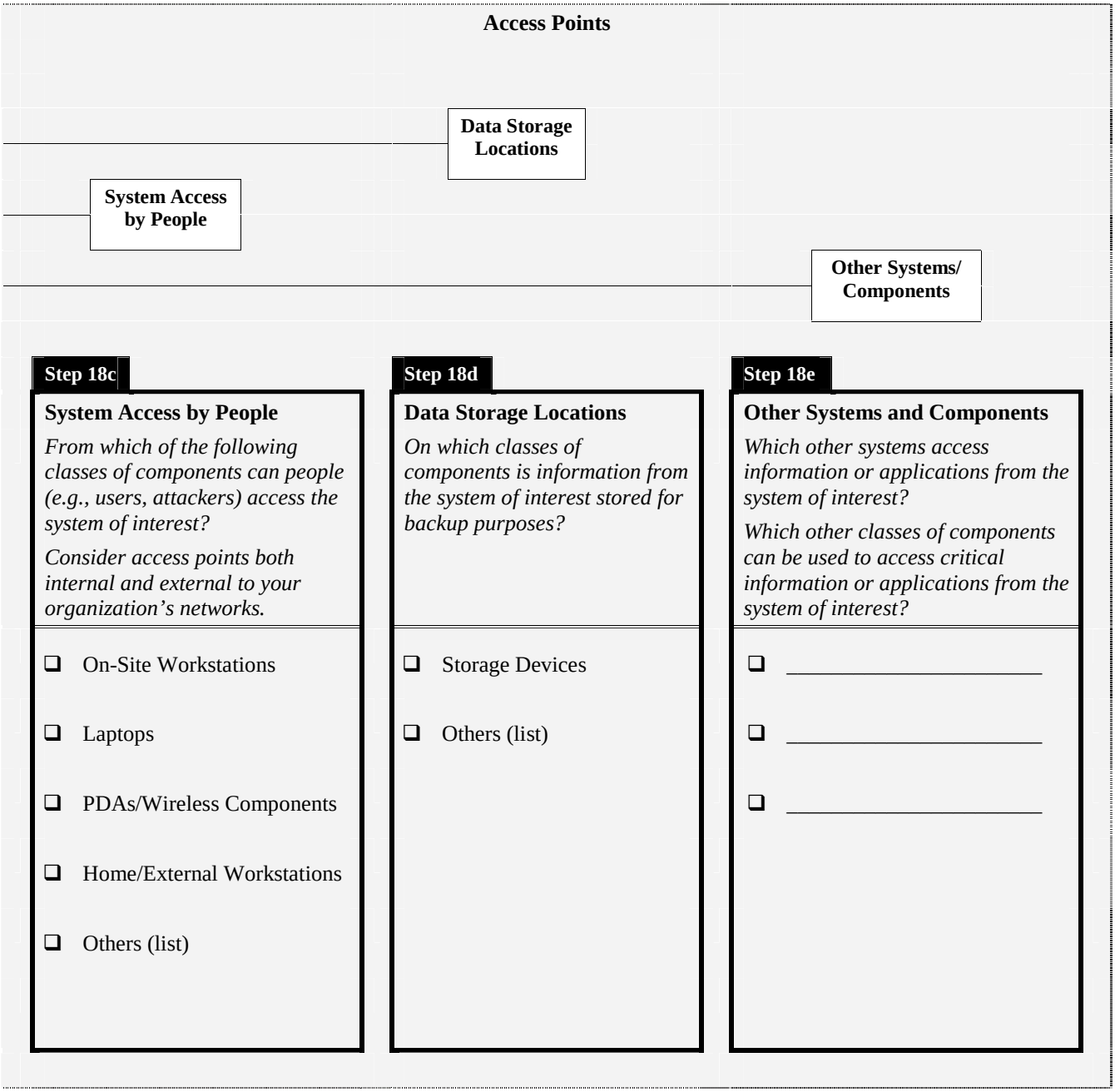
Intermediate Access Points

Which of the following classes of components are used to transmit information and applications from the system of interest to people?

Which classes of components could serve as intermediate access points?

- ❑ Internal Networks
- ❑ External Networks
- ❑ Others (list)

***Note**: When you select a key class of components, make sure that you also document any relevant subclasses or specific examples when appropriate.*



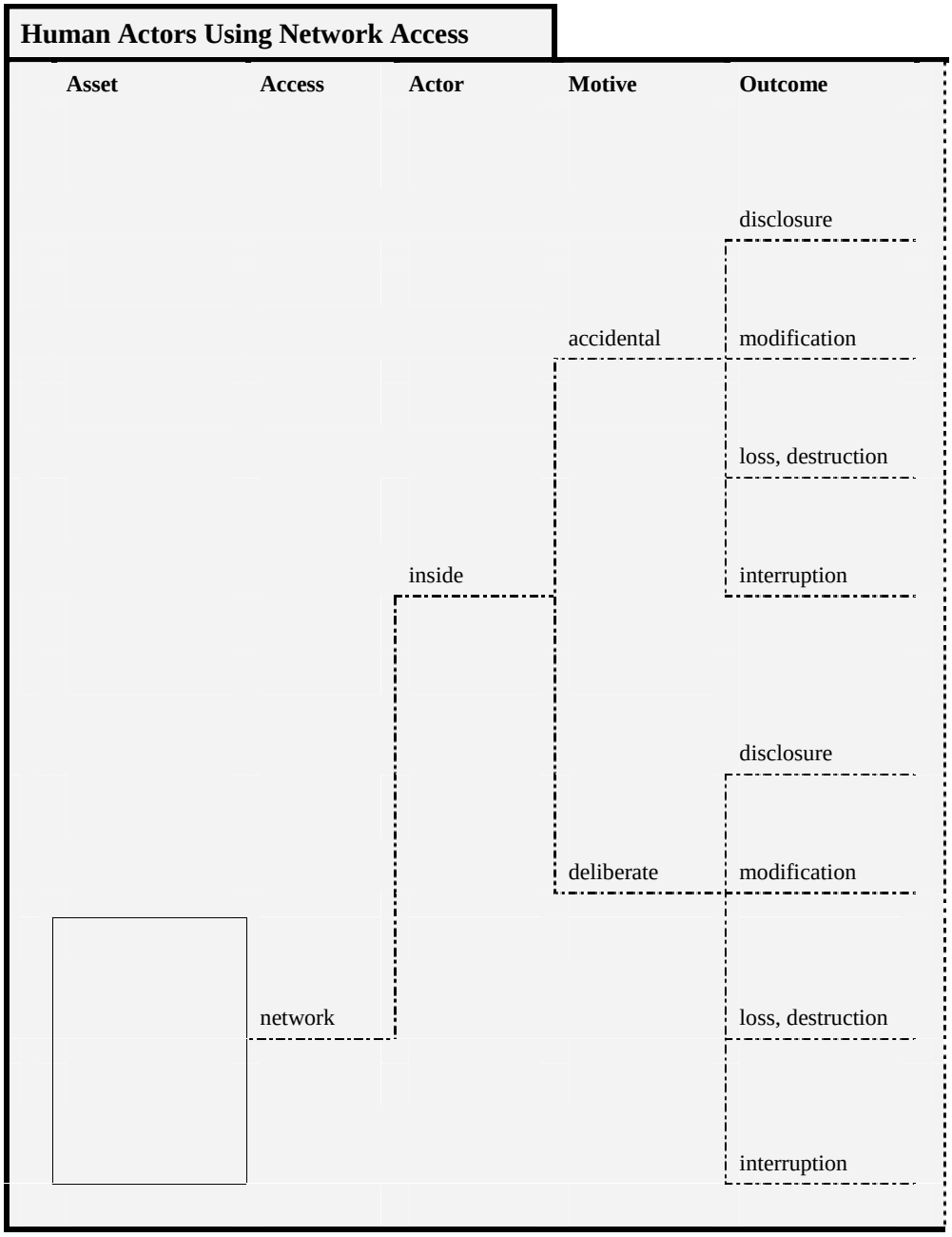
8 Threat Translation Guide

Phase 1
Process S2
Activity S2.3

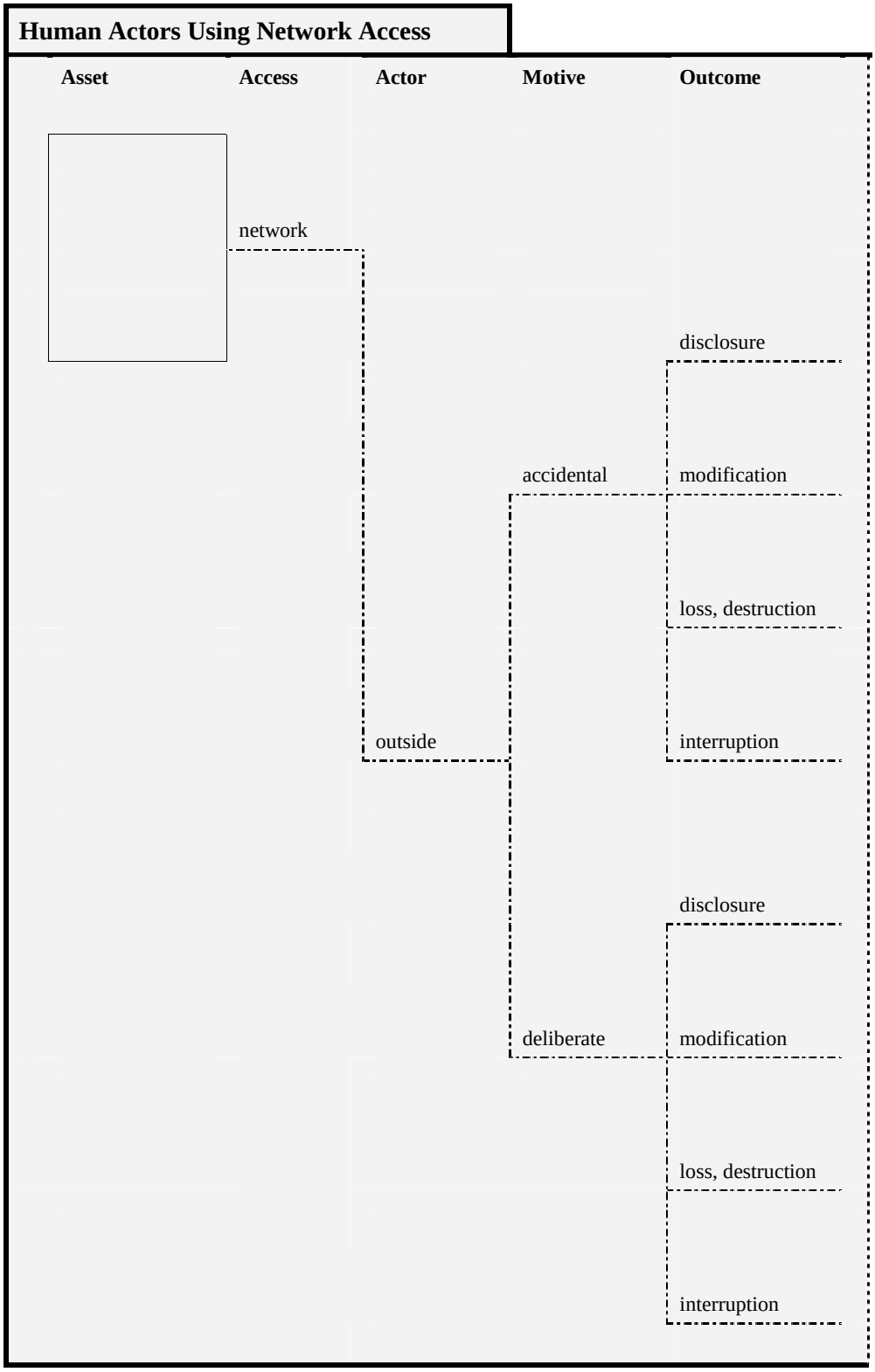
Threat Translation Guide

The *Threat Translation Guide* describes each branch of an asset-based threat tree. If you have difficulty understanding the types of threats represented by a branch, you can use this guide to decipher the meaning of that branch.

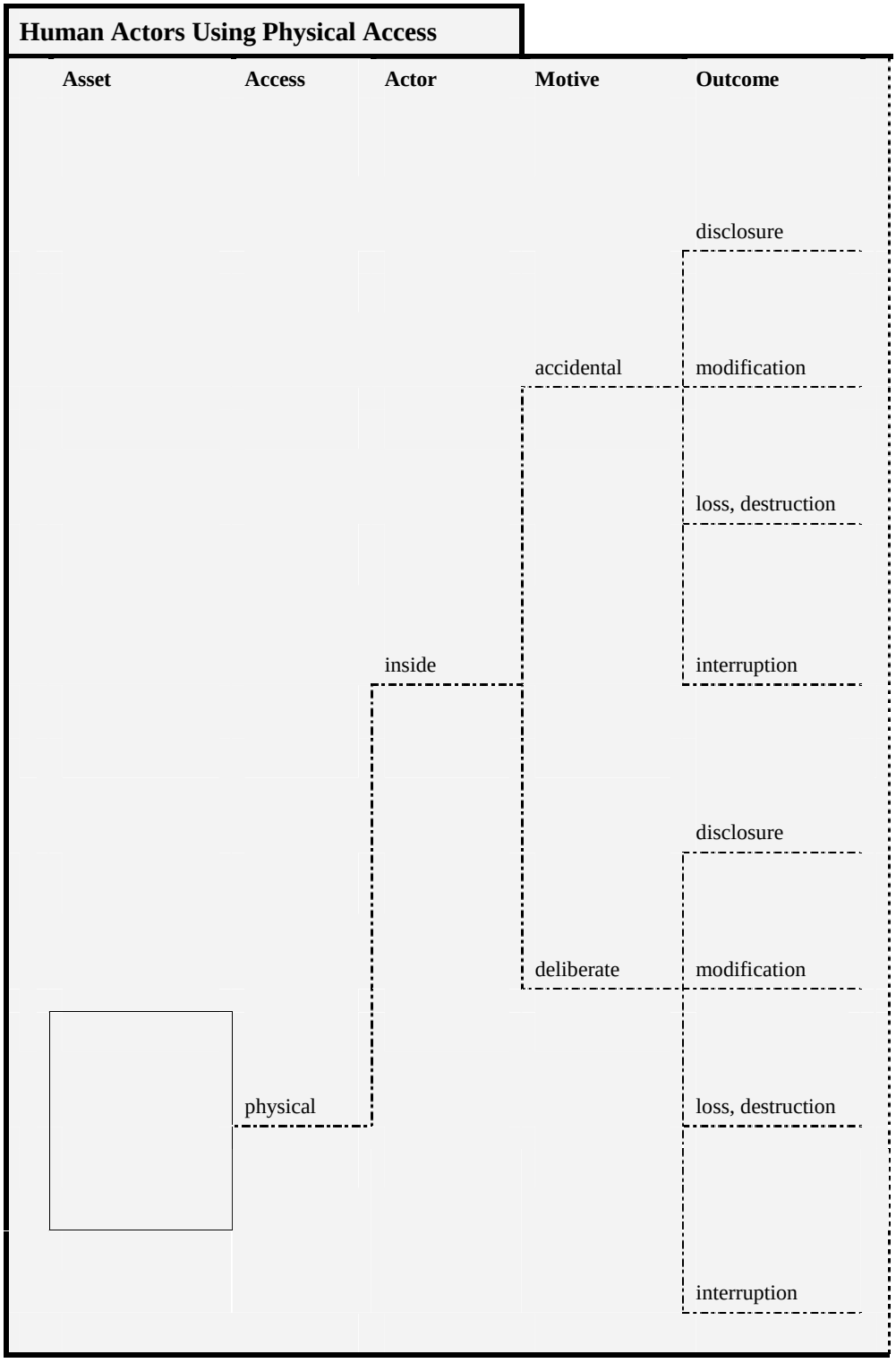
You will find asset-based threat trees for the following sources of threat:


Human Actors Using Network Access
Asset
Access
Actor
Motive
Outcome
disclosure
accidental
modification
loss, destruction
inside
interruption
disclosure
deliberate
modification
network
loss, destruction
interruption

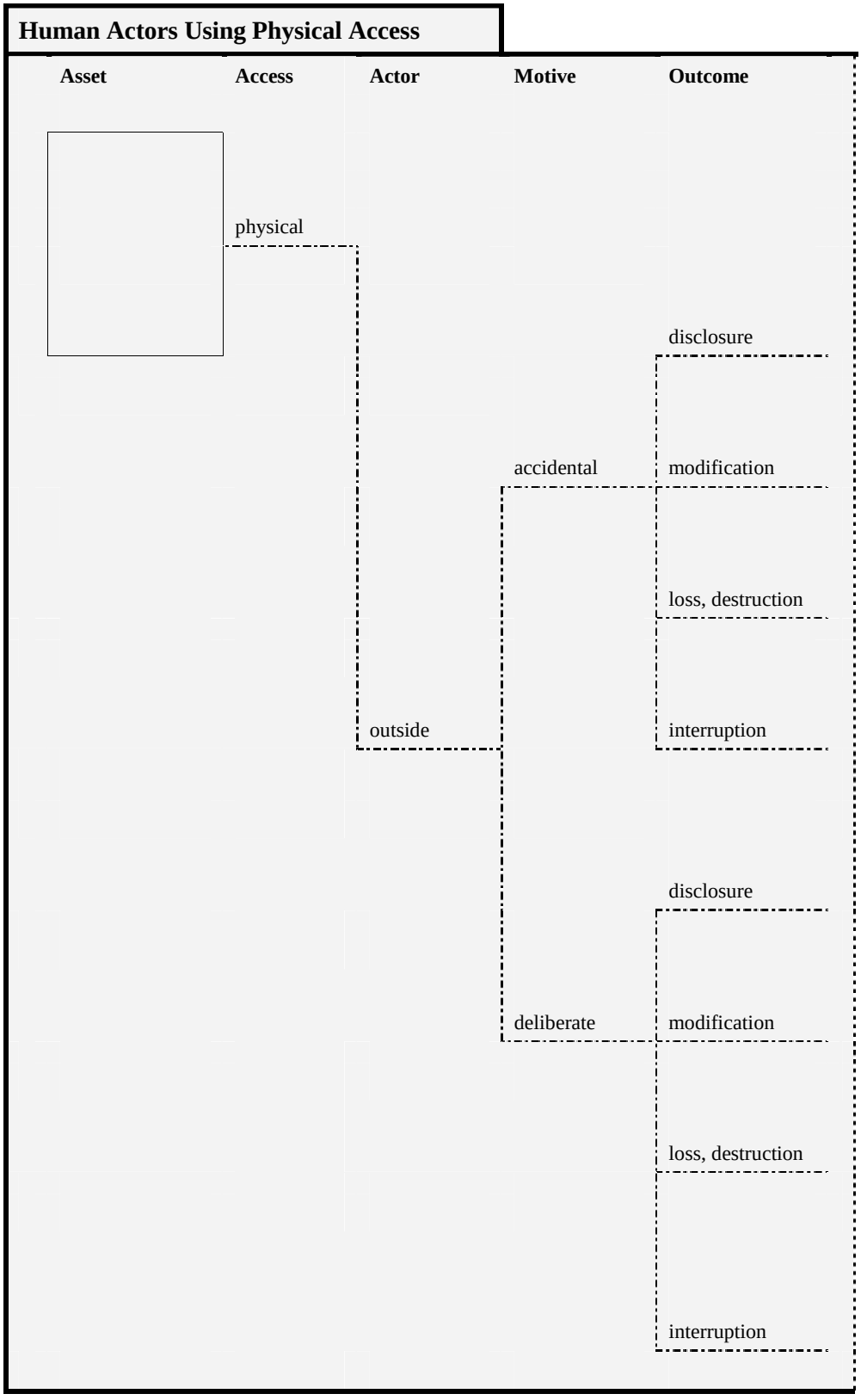
Description	Example
A staff member without malicious intent who has legitimate access to the computing infrastructure accidentally views confidential information on an important system.	Incorrect file permissions enable a staff member to accidentally access a restricted personnel database.
A staff member without malicious intent who has legitimate access to the computing infrastructure accidentally modifies information on an important system.	A staff member accidentally enters incorrect financial data into a customer database.
A staff member without malicious intent who has legitimate access to the computing infrastructure accidentally loses or destroys information on an important system.	A staff member deletes an important customer file by mistake.
A staff member without malicious intent who has legitimate access to the computing infrastructure accidentally interrupts access to an important system.	A staff member who is not computer savvy inadvertently crashes an important system.
A staff member with malicious intent who has legitimate access to the computing infrastructure exploits that access to deliberately view confidential information on an important system.	A staff member uses access to a restricted personnel database to deliberately view information in that database that is restricted by policy.
A staff member with malicious intent who has legitimate access to the computing infrastructure exploits that access to deliberately modify information on an important system.	A staff member responsible for data entry deliberately enters incorrect customer information into a database.
A staff member with malicious intent who has legitimate access to the computing infrastructure exploits that access to deliberately lose or destroy information on an important system.	A staff member with access to design documents for a new product deliberately deletes the files that contain those design documents.
A staff member with malicious intent who has legitimate access to the computing infrastructure exploits that access to deliberately interrupt access to an important system.	A staff member uses legitimate access to the computing infrastructure to launch a denial-of-service attack on an important system.


Human Actors Using Network Access
Asset
Access
Actor
Motive
Outcome
network
outside
accidental
deliberate
disclosure
modification
loss, destruction
interruption
disclosure
modification
loss, destruction
interruption

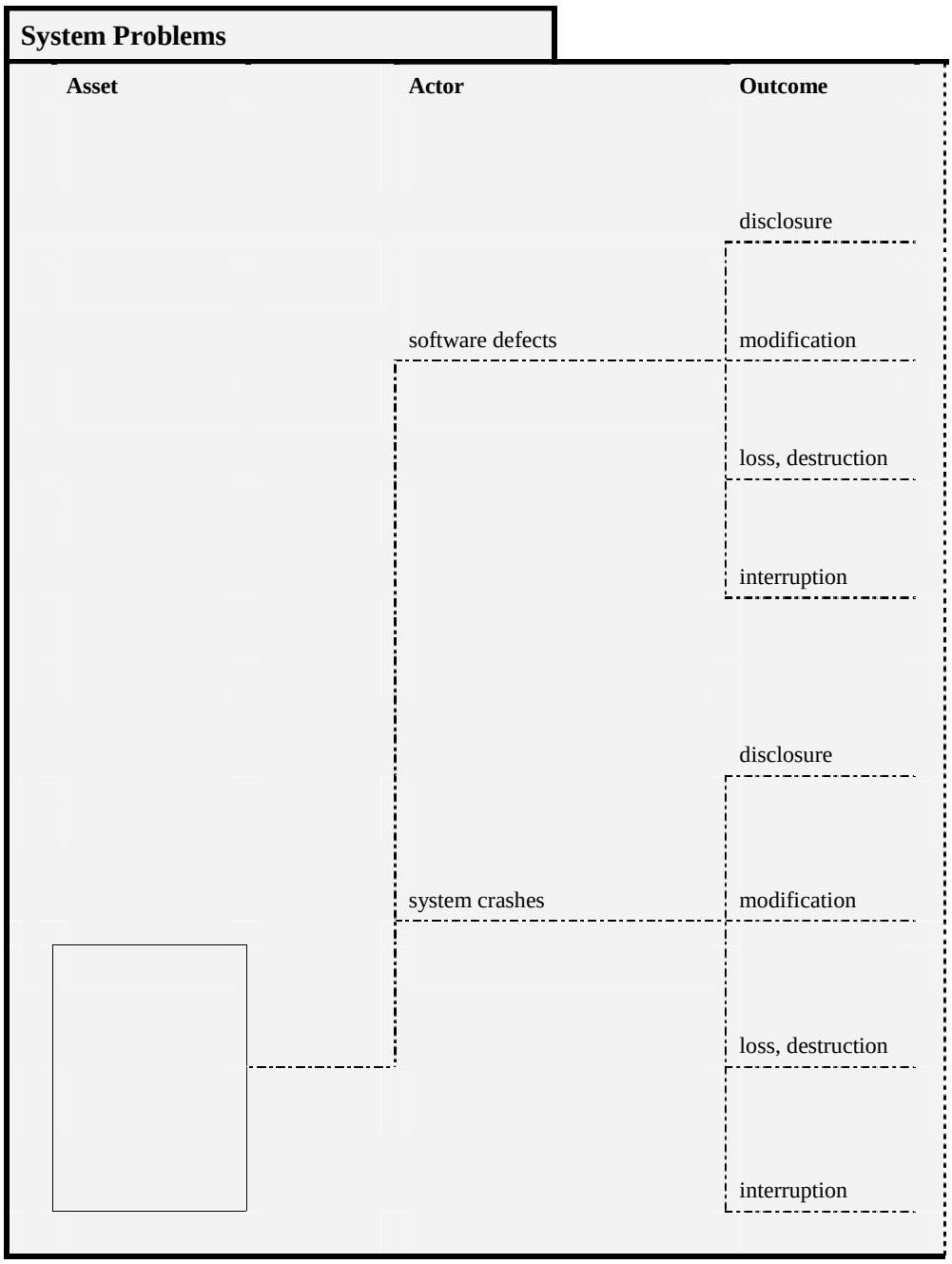
Description	Example
An outsider without malicious intent gains access to your computing infrastructure (legitimately or by accident) and views confidential data on a system.	Temporary employees are given access to your computing infrastructure to help with an increased workload. While performing their job duties, one of them accidentally views confidential personnel data.
An outsider without malicious intent gains access to your computing infrastructure (legitimately or by accident) and accidentally modifies information on a system.	Temporary employees are given access to your computing infrastructure to help with an increased workload. While performing their job duties, one of them accidentally modifies important customer data.
An outsider without malicious intent gains access to your computing infrastructure (legitimately or by accident) and loses or destroys information on a system.	Temporary employees are given access to your computing infrastructure to help with an increased workload. While performing their job duties, one of them accidentally loses or destroys financial data.
An outsider without malicious intent gains access to your computing infrastructure (legitimately or by accident) and accidentally interrupts access to a system.	Temporary employees are given access to your computing infrastructure to help with an increased workload. While performing their job duties, one of them accidentally crashes an important system.
An attacker with malicious intent deliberately exploits vulnerabilities in the computing infrastructure to view confidential information.	A corporate spy exploits vulnerabilities in the computing infrastructure to gain unauthorized access to a key business system. The spy uses that access to view confidential customer information on the system.
An attacker with malicious intent deliberately exploits vulnerabilities in the computing infrastructure to modify information.	A corporate spy exploits vulnerabilities in the computing infrastructure to gain unauthorized access to a key business system. The spy uses that access to modify financial data on the system.
An attacker with malicious intent deliberately exploits vulnerabilities in the computing infrastructure to lose or destroy information.	A corporate spy exploits vulnerabilities in the computing infrastructure to gain unauthorized access to a key business system. The spy uses that access to lose or destroy a new product design on the system.
An attacker with malicious intent deliberately exploits vulnerabilities in the computing infrastructure to interrupt access to a system.	A corporate spy exploits vulnerabilities in the computing infrastructure to gain unauthorized access to an airline's scheduling system. The spy uses that access to crash the system and prevent real-time updates.


Human Actors Using Physical Access
Asset
Access
Actor
Motive
Outcome
disclosure
accidental
modification
loss, destruction
inside
interruption
disclosure
deliberate
modification
physical
loss, destruction
interruption

Description	Example
A staff member without malicious intent accidentally views confidential information after gaining physical access to a system, one of its components, or a physical copy of the information.	A staff member accidentally sees confidential information on (1) a colleague's computer screen or (2) a printout on a colleague's desk.
A staff member without malicious intent accidentally modifies information after gaining physical access to a system, one of its components, or a physical copy of the information.	A staff member modifies information by (1) accidentally altering information on a colleague's computer while using it for another purpose or (2) accidentally taking a page of a printout on a colleague's desk.
A staff member without malicious intent accidentally loses or destroys information after gaining physical access to a system, one of its components, or a physical copy of the information.	A staff member loses or destroys information by (1) accidentally deleting information from a colleague's computer while using it or (2) shredding a paper accidentally taken from a colleague's desk.
A staff member without malicious intent interrupts access to a system or information by accidentally using physical access to a system, one of its components, or a physical copy of the information to prevent others from accessing the system or information.	A staff member interrupts access to a system by (1) accidentally crashing the system while accessing it from a colleague's computer or (2) locking the keys inside an office where a physical file is stored.
A staff member with malicious intent deliberately views confidential information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A staff member uses unauthorized access to a physically restricted area of the building to deliberately (1) view confidential information on a computer or (2) read a confidential memo lying on a desk.
A staff member with malicious intent deliberately modifies information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A staff member uses unauthorized access to a physically restricted area of the building to deliberately (1) modify information on a computer or (2) modify a physical file lying on a desk.
A staff member with malicious intent deliberately loses or destroys information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A staff member uses unauthorized access to a physically restricted area of the building to deliberately (1) delete information on a computer or (2) destroy a physical file lying on a desk.
A staff member with malicious intent deliberately interrupts access to an important system or information by breeching physical security to a system, one of its components, or a physical copy of the information and using that physical access to prevent others from accessing the system or information.	A staff member uses unauthorized access to a physically restricted area of the building to (1) gain access to and then deliberately crash an important business system or (2) jam the door and prevent others from physically accessing the systems and information located in that area of the building.

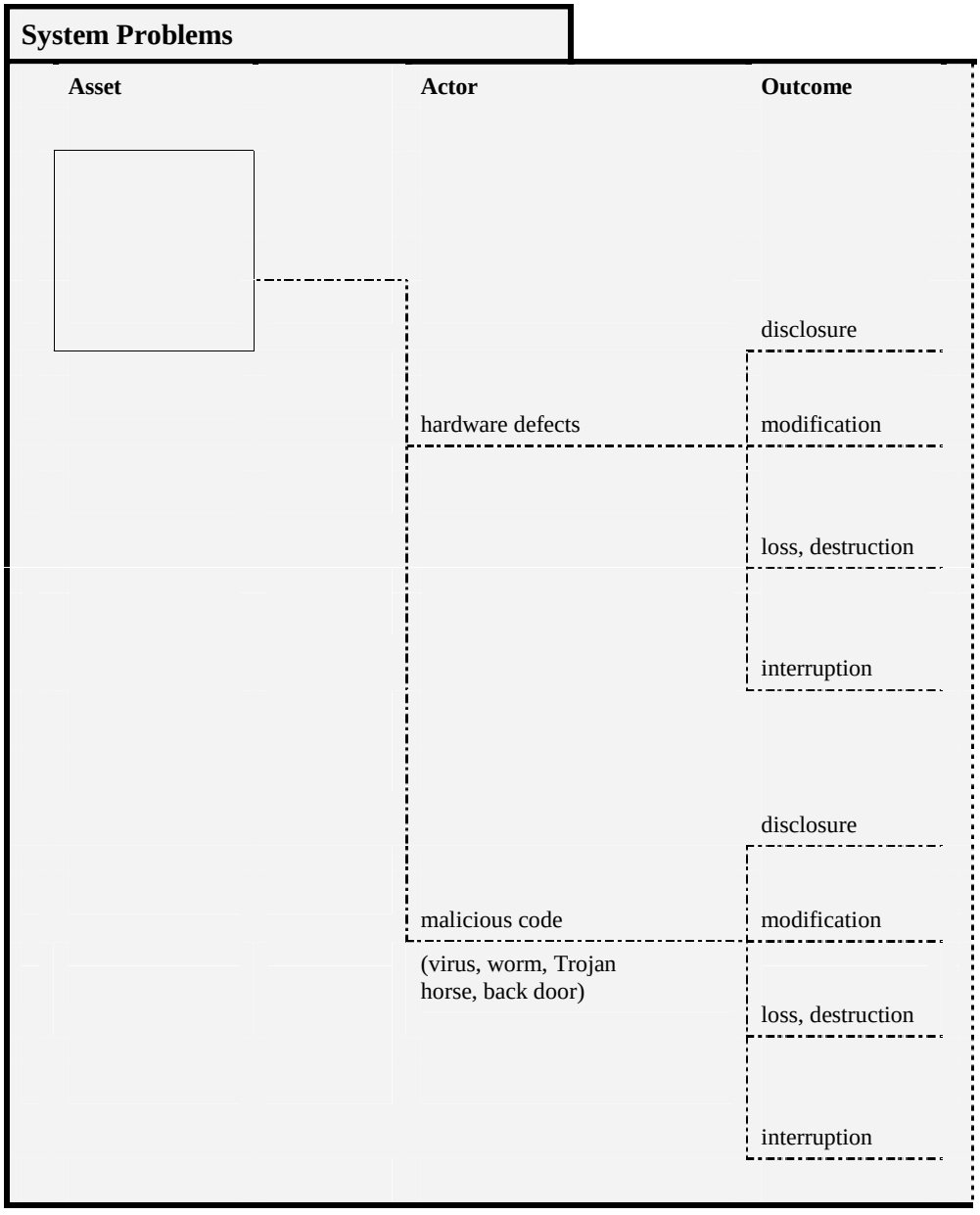

Human Actors Using Physical Access
Asset
Access
Actor
Motive
Outcome
physical
outside
accidental
disclosure
modification
loss, destruction
interruption
deliberate
disclosure
modification
loss, destruction
interruption

Description	Example
An outsider without malicious intent gains physical access to your computing infrastructure or a physical copy of information and uses that access to view confidential information accidentally.	A consultant is given access to a staff member's office and accidentally sees confidential information on (1) a staff member's computer screen or (2) a printout on a staff member's desk.
An outsider without malicious intent gains physical access to your computing infrastructure or a physical copy of information and uses that access to modify information accidentally.	A consultant is given access to the computer room and (1) accidentally makes the wrong change to a configuration file on a server or (2) accidentally records the wrong information in a maintenance log.
An outsider without malicious intent gains physical access to your computing infrastructure or a physical copy of information and uses that access to lose or destroy information accidentally.	A consultant configuring one of your servers is given access to the computer room and accidentally (1) destroys an important electronic file or (2) throws away an important piece of system documentation.
An outsider without malicious intent gains physical access to your computing infrastructure or a physical copy of information and uses that access to accidentally prevent others from accessing the information.	A consultant configuring one of your servers is given access to the computer room and accidentally (1) crashes a system while accessing it or (2) locks the keys to the computer room inside it after he or she leaves.
An attacker with malicious intent deliberately views confidential information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A corporate spy poses as a member of the cleaning crew to gain unauthorized physical access to a competitor's site and view confidential information either (1) on a key business system or (2) in a physical file.
An attacker with malicious intent deliberately modifies information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A corporate spy poses as a member of the cleaning crew to gain unauthorized physical access to a competitor's site and modify financial information either (1) on a key business system or (2) in a physical file.
An attacker with malicious intent deliberately loses or destroys information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A corporate spy poses as a member of the cleaning crew to gain unauthorized physical access to a competitor's site and destroy customer information either (1) on a key business system or (2) in a physical file.
An attacker with malicious intent deliberately interrupts access to an important system or information by breeching physical security to a system, one of its components, or a physical copy of the information and by using that physical access to prevent others from accessing the system or information.	A corporate spy poses as a member of the cleaning crew to gain unauthorized physical access to a competitor's site and (1) deliberately crashes an important business system or (2) jams the door to prevent others from physically accessing the systems and information located in an area of the building.



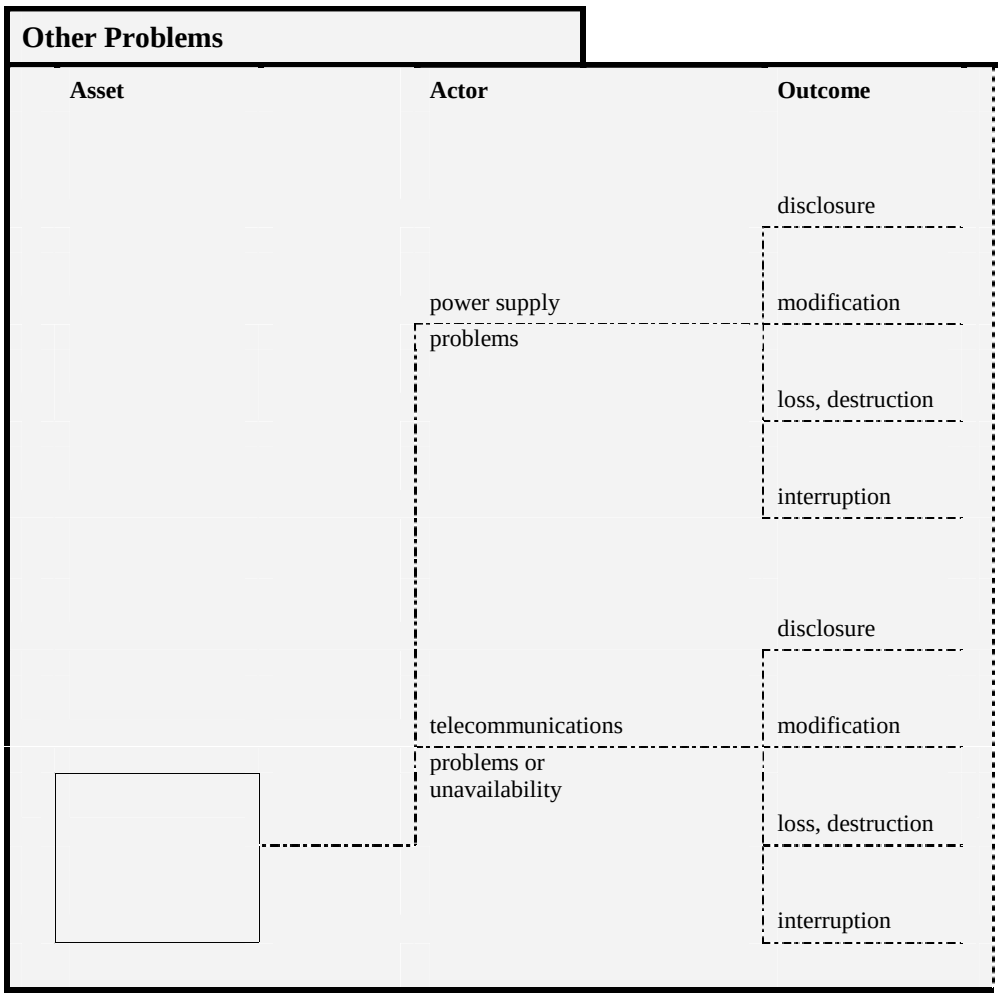
* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
A software defect results in disclosure of information to unauthorized parties.	A defect in a computer's operating system changes file access permissions to permit world read and write permissions on certain files and directories.
A software defect results in modification of information on a system.	A custom software application incorrectly performs mathematical operations on data, affecting the integrity of the results.
A software defect results in the loss or destruction of information on a system.	A word processing application is known to crash computers periodically because of a problem with a specific command sequence, destroying any information that was not saved.
A software defect results in a system crash, preventing access to the system.	A word processing application is known to crash computers periodically because of a problem with a specific command sequence, preventing access to that computer.
A system crashes for unknown reasons (i.e., it cannot be traced to a software defect, hardware defect, malicious code, or actions by people), resulting in disclosure of information to unauthorized parties.	---
A system crashes for unknown reasons (i.e., it cannot be traced to a software defect, hardware defect, malicious code, or actions by people), resulting in modification of information on that system.	A system crashes during a lengthy update of a financial database, corrupting the information in the database.
A system crashes for unknown reasons (i.e., it cannot be traced to a software defect, hardware defect, malicious code, or actions by people), resulting in the loss or destruction of information on that system.	A customer database system frequently crashes, destroying any information that was not saved at the time of the crash.
A system crashes for unknown reasons (i.e., it cannot be traced to a software defect, hardware defect, malicious code, or actions by people), resulting in interruption of access to that system.	An email server crashes, resulting in interruption of user access to email.



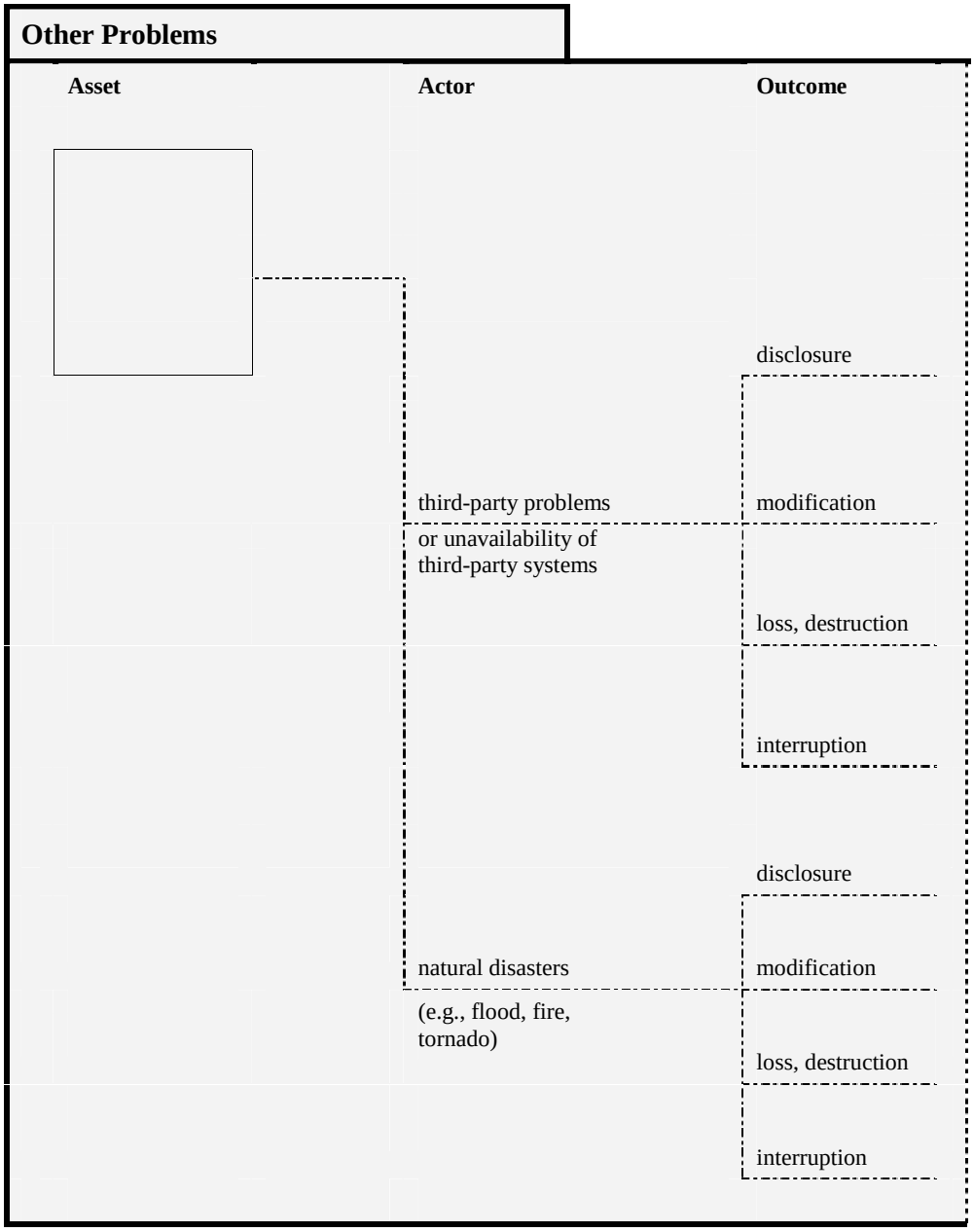
* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
A hardware defect results in disclosure of information to unauthorized parties.	---
A hardware defect results in modification of information on a system.	A disk drive develops a hardware problem that affects the integrity of a database that is stored on the disk.
A hardware defect results in the loss or destruction of information on a system.	A disk drive develops a hardware problem that ends up destroying the information on the disk. Files can be retrieved only from backups.
A hardware defect results in a system crash, preventing access to the system.	A disk drive develops a hardware problem, preventing access to any information on the disk until the problem is corrected.
A system is affected by malicious code (virus, worm, Trojan horse, back door) that enables unauthorized parties to view information.	A back door on a system enables unauthorized people to access the system and view customer credit card information on that system.
A system is affected by malicious code (virus, worm, Trojan horse, back door) that modifies information on that system.	A system is infected with a virus that modifies a process control application on the computer's disk drive.
A system is affected by malicious code (virus, worm, Trojan horse, back door) that deletes information on that system.	A system is infected with a virus that deletes all information on the computer's disk drive.
A system is affected by malicious code (virus, worm, Trojan horse, back door) that results in the system crashing.	A system is infected with a virus that is spread via email, slowing network traffic and creating a denial-of-services attack.



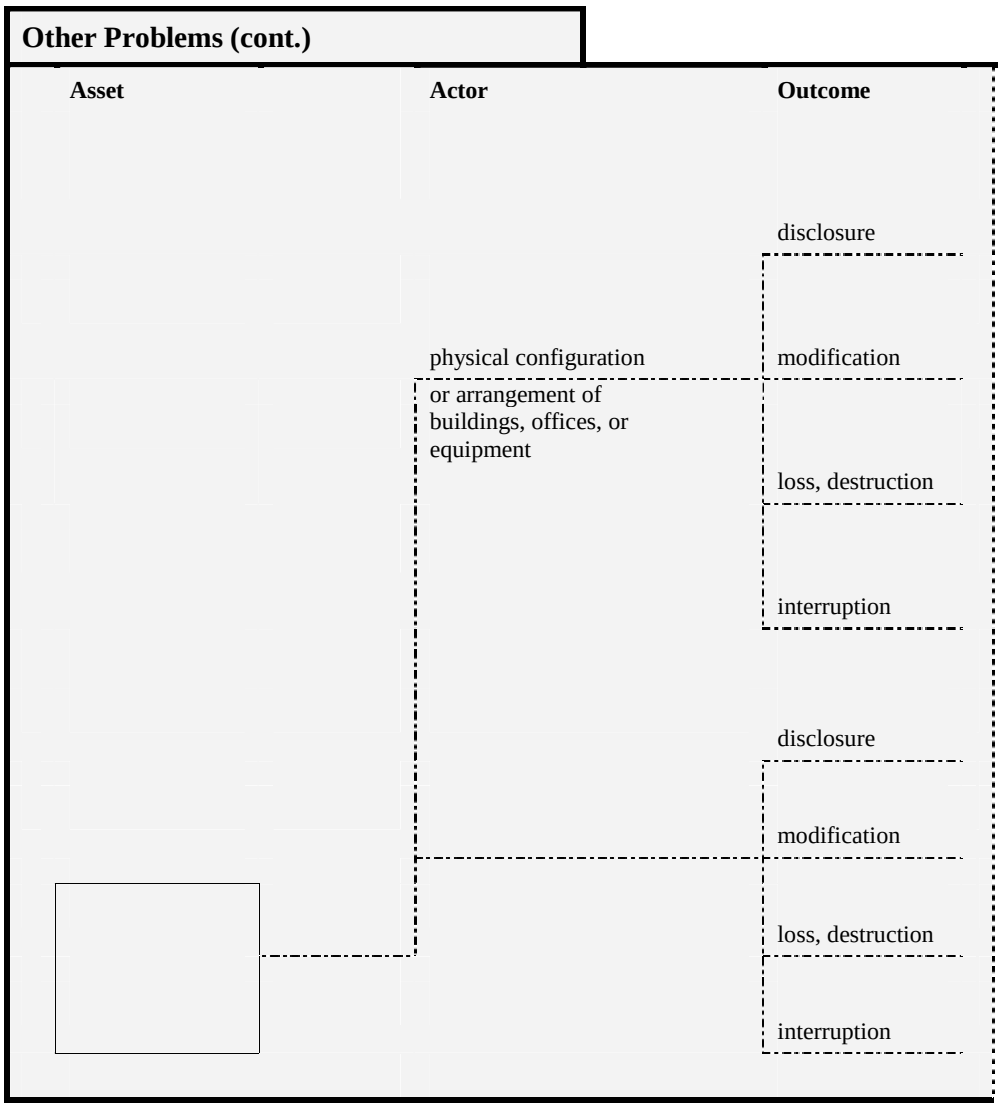
* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
Problems with the power supply lead to disclosure of information to unauthorized parties.	---
Problems with the power supply lead to modification of information on a system.	---
Problems with the power supply lead to loss or destruction of information on a system.	A power outage results in loss of any information that was not saved at the time of the outage.
Problems with the power supply lead to interruption of access to a system.	A power outage prevents access to all key business systems.
Unavailability of telecommunications services leads to disclosure of information to unauthorized parties.	---
Unavailability of telecommunications services leads to modification of information on a system.	---
Unavailability of telecommunications services leads to loss or destruction of information on a system.	---
Unavailability of telecommunications services leads to interruption of access to a system.	The unavailability of the telecommunications link prevents access to a key business system located at a remote site.



* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
Problems with services provided by third parties (e.g., maintenance of systems) lead to disclosure of information to unauthorized parties.	A staff member from a third-party service provider views confidential information on a key business system that is maintained by that service provider.
Problems with services provided by third parties (e.g., maintenance of systems) lead to modification of information on a system.	Problems at a third-party service provider lead to the modification of information on a key business system located at that provider's site and maintained by the provider.
Problems with services provided by third parties (e.g., maintenance of systems) lead to loss or destruction of information on a system.	Problems at a third-party service provider lead to the destruction of information on a key business system located at that provider's site and maintained by the provider.
Problems with services provided by third parties (e.g., maintenance of systems) lead to interruption of access to a system.	A system maintained by a third-party service provider and located at the provider's site is unavailable due to problems created by that provider's staff.
Natural disasters (e.g., flood, fire, tornado) lead to disclosure of information to unauthorized parties.	People at the site of a tornado see confidential memos that are dispersed among the debris.
Natural disasters (e.g., flood, fire, tornado) lead to modification of information.	---
Natural disasters (e.g., flood, fire, tornado) lead to loss or destruction of information.	The flooding of a basement area destroys paper records that are stored there.
Natural disasters (e.g., flood, fire, tornado) lead to interruption of access to a system.	The flooding of a computer room in the basement of a building prevents access to systems in that room.



* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
The physical configuration or arrangement of buildings, offices, or equipment leads to disclosure of information to unauthorized parties.	The layout of an office workspace enables anyone in the area to view customer credit card information displayed on computer screens.
The physical configuration or arrangement of buildings, offices, or equipment leads to modification of information on a system.	---
The physical configuration or arrangement of buildings, offices, or equipment leads to loss or destruction of information on a system.	---
The physical configuration or arrangement of buildings, offices, or equipment leads to interruption of access to a system.	---

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
OCTAVE-S Implementation Guide, Version 1.0, Volume 6	F19628-00-C-0003

6. AUTHOR(S)

Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody

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

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

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

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

14. SUBJECT TERMS	15. NUMBER OF PAGES
information security, risk management, OCTAVE	78

16. PRICE CODE

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

OCTAVE®-S Implementation Guide, Version 1.0

Volume 7: Critical Asset Worksheets for Applications

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

HANDBOOK
CMU/SEI-2003-HB-003

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

OCTAVE®-S Implementation Guide, Version 1.0

Volume 7: Critical Asset Worksheets for Applications

CMU/SEI-2003-HB-003

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

Networked Systems Survivability Program

This report was prepared for the

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

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

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

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

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

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

Table of Contents

List of Tables

About This Document

This document is Volume 6 of the *OCTAVE-S Implementation Guide*, a 10-volume handbook supporting the OCTAVE-S methodology. This volume provides worksheets to document data related to critical assets that are categorized as applications.

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 Introduction

This document contains the Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE[®])-S worksheets related to critical assets that are applications. The activities related to these worksheets are focused on analyzing a critical asset.

Table 1 provides a brief introduction to the contents of this workbook, using activity step numbers as a key. For more details about how to complete each step, refer to the *OCTAVE®-S Method Guidelines*, which can be found in Volume 3 of the *OCTAVE®-S Implementation Guide*.

Table 1: Worksheets Provided in This Workbook

Step	Description	Worksheet	Activity	Pages
Step 6	Start a *Critical Asset Information worksheet* for each critical asset. Record the name of the critical asset on its *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 7	Record your rationale for selecting each critical asset on that asset's *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 8	Record a description for each critical asset on that asset's *Critical Asset Selection worksheet*. Consider who uses each critical asset as well as who is responsible for it.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 9	Record assets that are related to each critical asset on that asset's *Critical Asset Information worksheet*. Refer to the *Asset Identification worksheet* to determine which assets are related to each critical asset.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8

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

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

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 10	Record the security requirements for each critical asset on that asset's *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 11	For each critical asset, record the most important security requirement on that asset's *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 12	Complete all appropriate threat trees for each critical asset. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on any threat tree, review the description and examples of that threat in the *Threat Translation Guide*.	Risk Profile Threat Translation Guide	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-54
Step 13	Record specific examples of threat actors on the *Risk Profile worksheet* for each applicable actor-motive combination.	Risk Profile	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-54
Step 14	Record the strength of the motive for deliberate threats due to human actors. Also record how confident you are in your estimate of the strength of the actor's motive.	Risk Profile	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-54
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.	Risk Profile	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-54
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.	Risk Profile	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-54

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 17	Select the system of interest for each critical asset (i.e., the system most closely related to the critical asset).	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58
Step 18a	Review paths used to access each critical asset, and select key classes of components related to each critical asset. Determine which classes of components are part of the system of interest.	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58
Step 18b	Determine which classes of components serve as intermediate access points (i.e., which components are used to transmit information and applications from the system of interest to people).	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58
Step 18c	Determine which classes of components, both internal and external to the organization's networks, are used by people (e.g., users, attackers) to access the system.	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58
Step 18d	Determine where information from the system of interest is stored for backup purposes.	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58
Step 18e	Determine which other systems access information or applications from the system of interest and which other classes of components can be used to access critical information or services from the system of interest.	Network Access Paths	Phase 2 Process S3 S3.1 Examine Access Paths	55-58

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) for each active threat to each critical asset.	Risk Profile Impact Evaluation Criteria	Phase 3 Process S4 S4.1 Evaluate Impacts of Threats	9-54
Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) for each active threat to each critical asset. Document your confidence level in your probability estimate.	Risk Profile Probability Evaluation Criteria	Phase 3 Process S4 S4.3 Evaluate Probabilities of Threats	9-54
Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of each critical asset's *Risk Profile worksheet*.	Risk Profile Security Practices	Phase 3 Process S5 S5.2 Select Mitigation Approaches	9-54
Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.	Risk Profile	Phase 3 Process S5 S5.2 Select Mitigation Approaches	9-54

2 Critical Asset Information Worksheet for Applications

	Phase 1 **Process S2** **Activity S2.1**
Step 6	Start a *Critical Asset Information worksheet* for each critical asset. Record the name of the critical asset on its *Critical Asset Information worksheet*.
Step 7	Record your rationale for selecting each critical asset on that asset's *Critical Asset Information worksheet*.
Step 8	Record a description for each critical asset on that asset's *Critical Asset Selection worksheet*. Consider who uses each critical asset as well as who is responsible for it.
Step 9	Record assets that are related to each critical asset on that asset's *Critical Asset Information worksheet*. Refer to the *Asset Identification worksheet* to determine which assets are related to each critical asset.
	Phase 1 **Process S2** **Activity S2.2**
Step 10	Record the security requirements for each critical asset on that asset's *Critical Asset Information worksheet*.
Step 11	For each critical asset, record the most important security requirement on that asset's *Critical Asset Information worksheet*.

Step 6	Step 7
Critical Asset	**Rationale for Selection**
What is the critical application?	*Why is this application critical to the organization?*

Step 9
Related Assets
Which assets are related to this application?
Systems: Information:
Other:

Step 8

Description	
Who uses the application?	*Who is responsible for the application?*

Step 10

Security Requirements		**Step 11** **Most Important Security Requirement**
What are the security requirements for this application? *(Hint: Focus on what the security requirements should be for this application, not what they currently are.)*		*Which security requirement is most important for this application?*
❑ Confidentiality	Only authorized personnel can view _____.	❑ Confidentiality
❑ Integrity	Only authorized personnel can modify _____ (e.g., install new versions, upgrade the service or application).	❑ Integrity
❑ Availability	_____ must be available for personnel to perform their jobs. Unavailability cannot exceed _____ hour(s) per every _____ hours.	❑ Availability
❑ Other	_____ _____	❑ Other

3 Risk Profile Worksheet for Applications – Human Actors Using Network Access

Phase 1
Process S2
Activity S2.3

Step 12	Complete the threat tree for *human actors using network access*. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on the threat tree, review the description and examples of that threat in the *Threat Translation Guide* (see pp. 60-63 of this workbook).
Step 13	Record specific examples of threat actors on the *Risk Profile worksheet* for each applicable actor-motive combination.
Step 14	Record the strength of the motive for deliberate threats due to human actors. Also record how confident you are in your estimate of the strength of the actor's motive.
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.

continued

	Phase 3 **Process S4** **Activity S4.1**
Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) to each active threat.

	Phase 3 **Process S4** **Activity S4.3**
Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) to each active threat. Document your confidence level in your probability estimate.

	Phase 3 **Process S5** **Activity S5.2**
Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of the following worksheet.

Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.

Human Actors Using Network Access **Basic Risk Profile**

Step 12

Threat

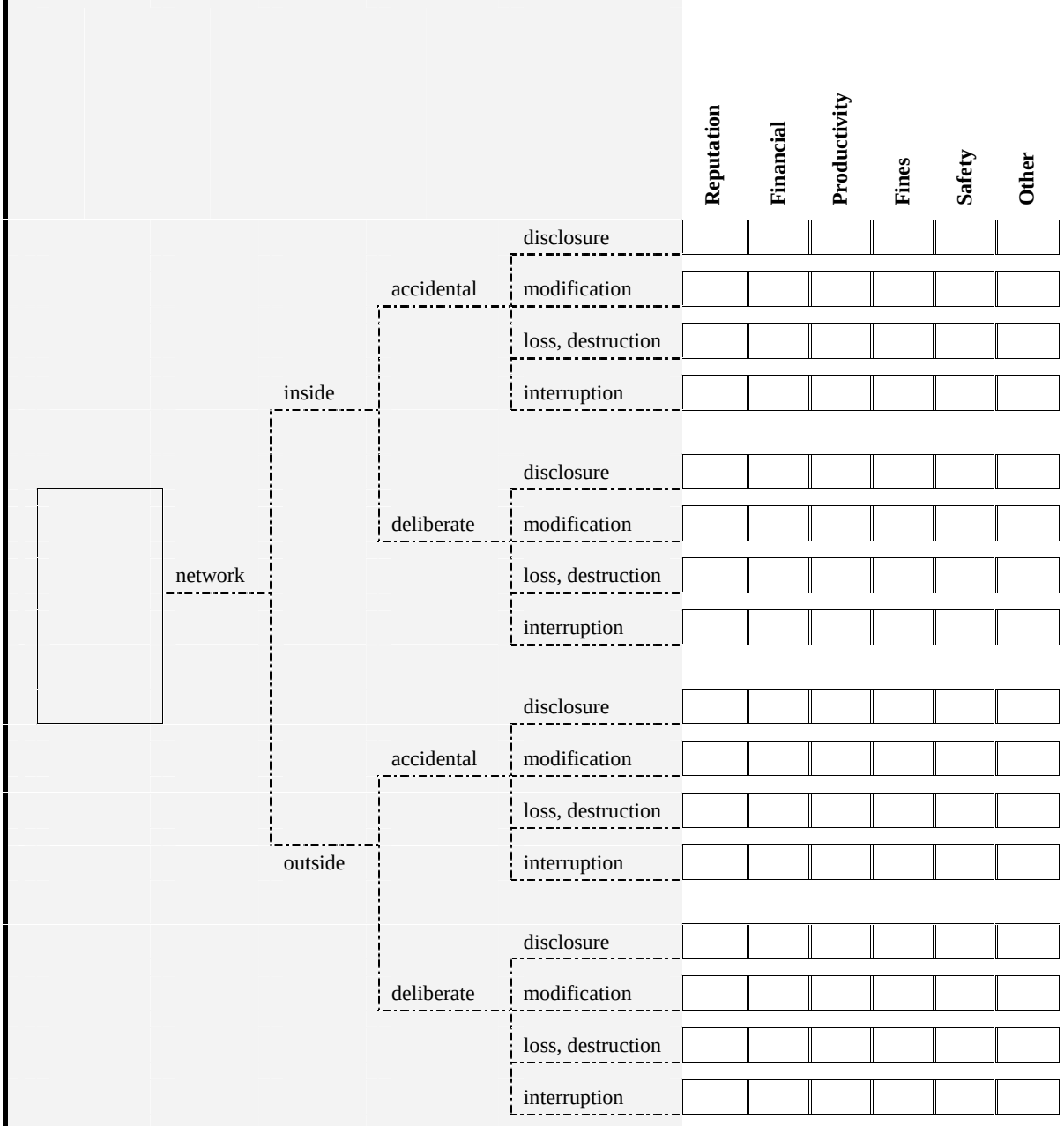
For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Step 22

Impact Values

What is the potential impact on the organization in each applicable area?



Basic Risk Profile | **Human Actors Using Network Access**

Step 24

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value	Confidence	
	Very	
	Somewhat	
	Not At All	

Step 26

Security Practice Areas

What is the stoplight status for each security practice area?

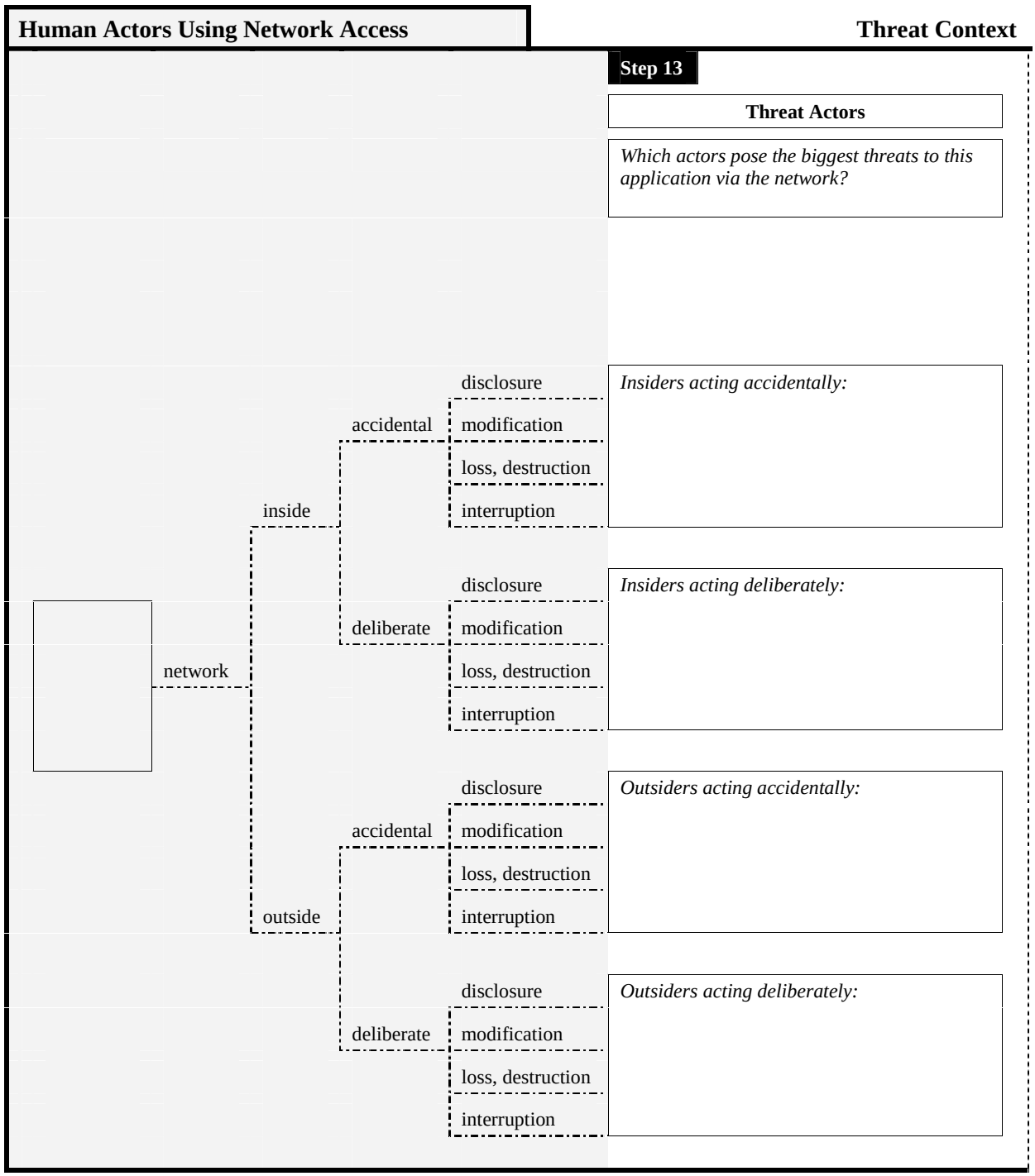
	Strategic						Operational								
	1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt
	--------														

Step 27

Approach

What is your approach for addressing each risk?

Accept	Defer	Mitigate
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑


Human Actors Using Network Access
Threat Context
Step 13
Threat Actors
Which actors pose the biggest threats to this application via the network?
network
inside
outside
accidental
deliberate
disclosure
modification
loss, destruction
interruption
Insiders acting accidentally:
Insiders acting deliberately:
Outsiders acting accidentally:
Outsiders acting deliberately:

Threat Context | **Human Actors Using Network Access**

Step 14 | **Step 15**

Motive						History			
How strong is the actor's motive?			*How confident are you in this estimate?*			*How often has this threat occurred in the past?*	*How accurate are the data?*		
High	**Medium**	**Low**	**Very**	**Somewhat**	**Not At All**		**Very**	**Somewhat**	**Not At All**
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑

Step 16

Human Actors Using Network Access	Areas of Concern

Insiders Using Network Access

Give examples of how *insiders acting accidentally* could use network access to threaten this application.	
Give examples of how *insiders acting deliberately* could use network access to threaten this application.	

Outsiders Using Network Access

Give examples of how *outsiders acting accidentally* could use network access to threaten this application.	
Give examples of how *outsiders acting deliberately* could use network access to threaten this application.	

Areas of Concern

Insiders Using Network Access

Outsiders Using Network Access

4 Risk Profile Worksheet for Applications – Human Actors Using Physical Access

Phase 1
Process S2
Activity S2.3

Step 12	Complete the threat tree for *human actors using physical access*. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on the threat tree, review the description and examples of that threat in the *Threat Translation Guide* (see pp. 64-67 of this workbook).
Step 13	Record specific examples of threat actors on the *Risk Profile worksheet* for each applicable actor-motive combination.
Step 14	Record the strength of the motive for deliberate threats due to human actors. Also record how confident you are in your estimate of the strength of the actor's motive.
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.

continued

	Phase 3 **Process S4** **Activity S4.1**
Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) to each active threat.

	Phase 3 **Process S4** **Activity S4.3**
Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) to each active threat. Document your confidence level in your probability estimate.

	Phase 3 **Process S5** **Activity S5.2**
Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of the following worksheet.

Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.

Human Actors Using Physical Access **Basic Risk Profile**

Step 12

Threat

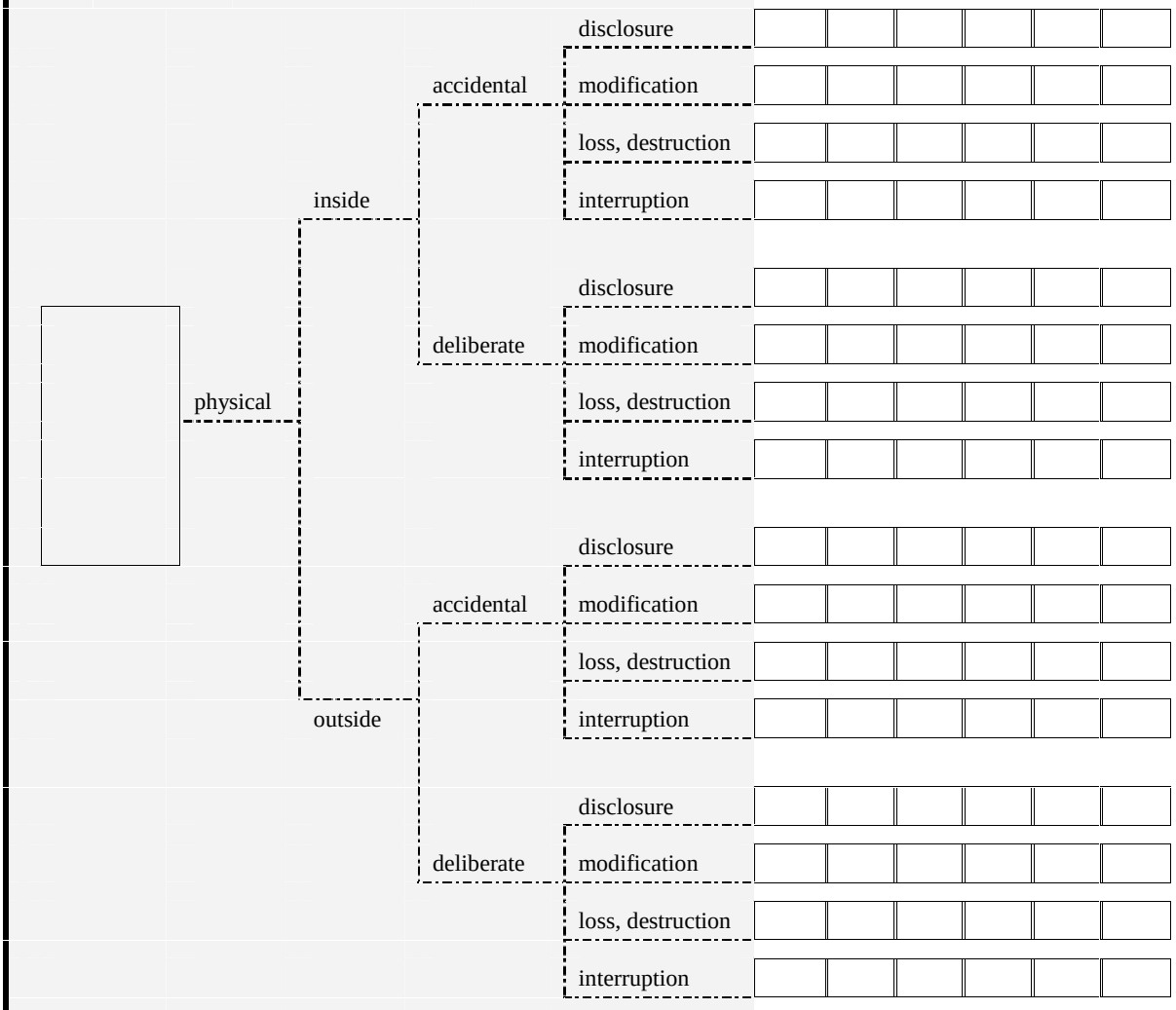
For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Step 22

Impact Values

What is the potential impact on the organization in each applicable area?



Basic Risk Profile | **Human Actors Using Physical Access**

Step 24 | **Step 26** | **Step 27**

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value **Confidence**

Security Practice Areas

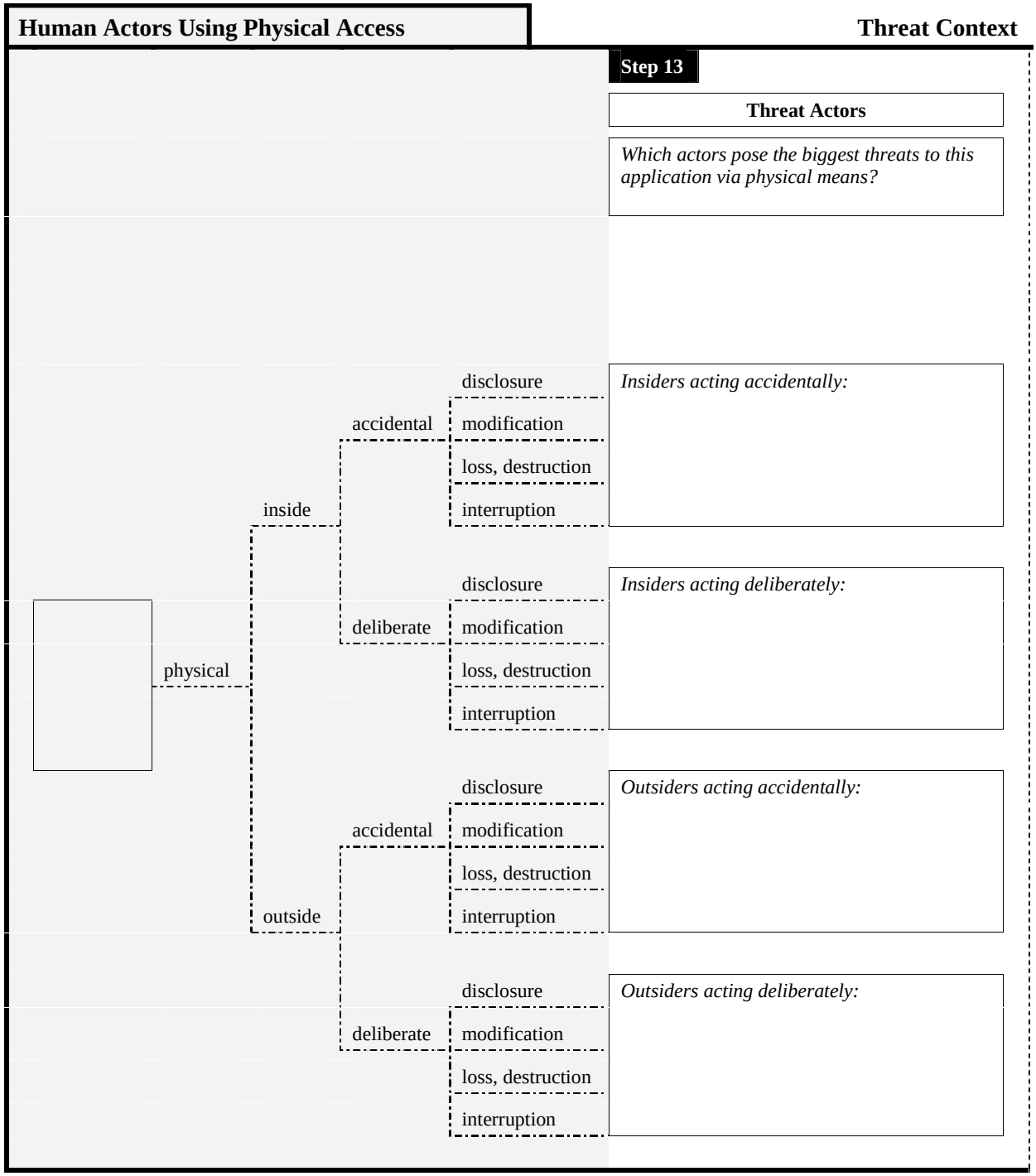
What is the stoplight status for each security practice area?

Strategic | **Operational**

Approach

What is your approach for addressing each risk?

Value	Confidence	1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt	Accept	Defer	Mitigate
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑
	Very / Somewhat / Not At All																❑	❑	❑


Human Actors Using Physical Access
Threat Context
Step 13
Threat Actors
Which actors pose the biggest threats to this application via physical means?
physical
inside
outside
accidental
deliberate
disclosure
modification
loss, destruction
interruption
Insiders acting accidentally:
Insiders acting deliberately:
Outsiders acting accidentally:
Outsiders acting deliberately:

Threat Context | **Human Actors Using Physical Access**

Step 14 | **Step 15**

Motive						History			
How strong is the actor's motive?			*How confident are you in this estimate?*			*How often has this threat occurred in the past?*	*How accurate are the data?*		
High	**Medium**	**Low**	**Very**	**Somewhat**	**Not At All**		**Very**	**Somewhat**	**Not At All**
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
						_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑
❑	❑	❑	❑	❑	❑	_____ times in _____ years	❑	❑	❑

Step 16

Human Actors Using Physical Access	Areas of Concern

Insiders Using Physical Access

Give examples of how *insiders acting accidentally* could use physical access to threaten this application.	
Give examples of how *insiders acting deliberately* could use physical access to threaten this application.	

Outsiders Using Physical Access

Give examples of how *outsiders acting accidentally* could use physical access to threaten this application.	
Give examples of how *outsiders acting deliberately* could use physical access to threaten this application.	

Areas of Concern

Insiders Using Physical Access

Outsiders Using Physical Access

5 Risk Profile Worksheet for Applications – System Problems

Phase 1
Process S2
Activity S2.3

Step 12	Complete the threat tree for *system problems*. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on the threat tree, review the description and examples of that threat in the *Threat Translation Guide* (see pp. 68-71 of this workbook).
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.

continued

	Phase 3 **Process S4** **Activity S4.1**
Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) to each active threat.

	Phase 3 **Process S4** **Activity S4.3**
Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) to each active threat. Document your confidence level in your probability estimate.

	Phase 3 **Process S5** **Activity S5.2**
Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of the following worksheet.

Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.

System Problems | **Basic Risk Profile**

Step 12 | **Step 22**

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Impact Values

What is the potential impact on the organization in each applicable area?

Asset	Actor	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other
	software defects	disclosure						
		modification						
		loss, destruction						
		interruption						
	system crashes	disclosure						
		modification						
		loss, destruction						
		interruption						
	hardware defects	disclosure						
		modification						
		loss, destruction						
		interruption						
	malicious code (virus, worm, Trojan horse, back door)	disclosure						
		modification						
		loss, destruction						
		interruption						

Basic Risk Profile | **System Problems**

Step 24

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value	Confidence	
	Very	
	Somewhat	
	Not At All	

Step 26

Security Practice Areas

What is the stoplight status for each security practice area?

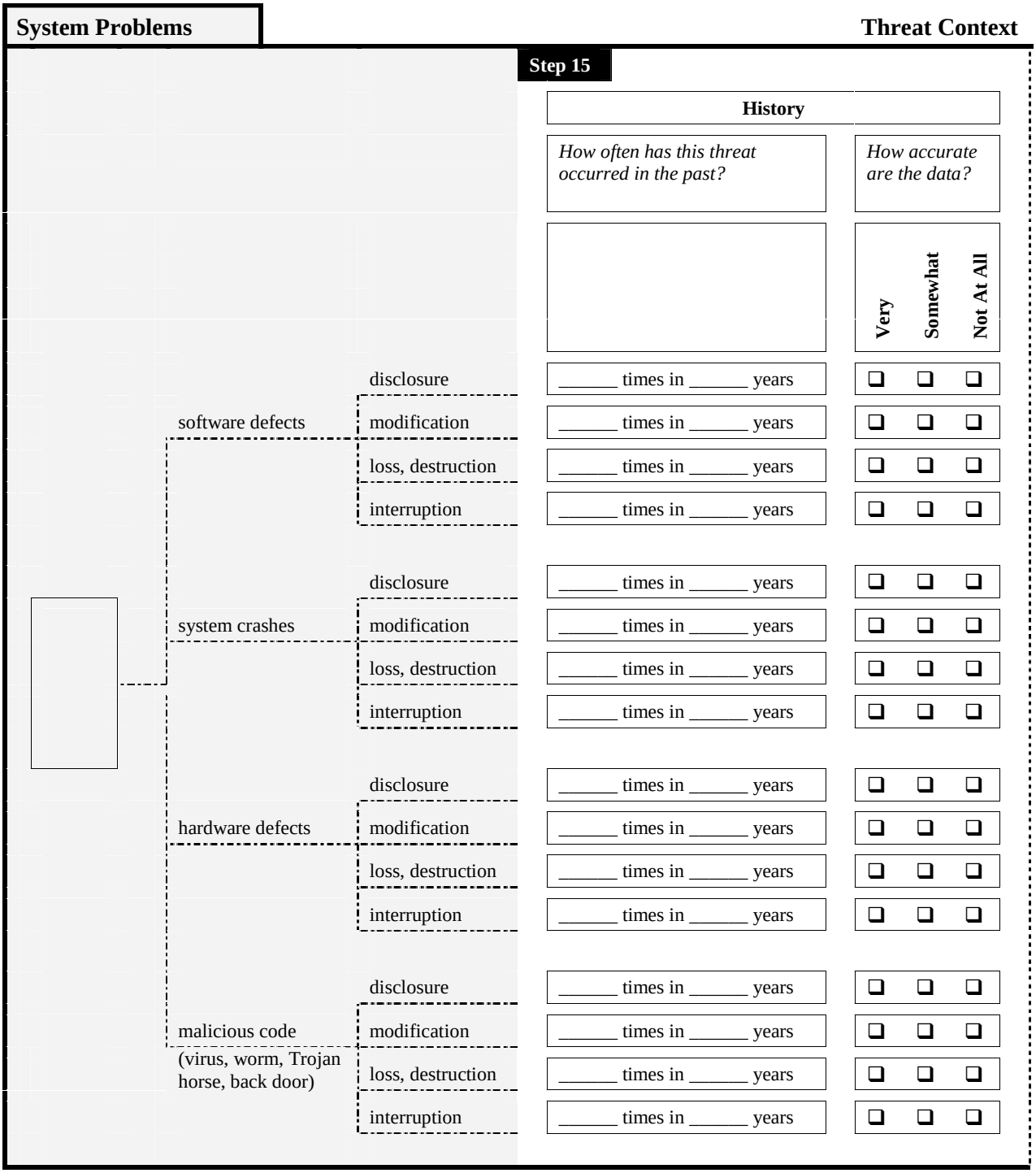
	Strategic						Operational								
	1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt

Step 27

Approach

What is your approach for addressing each risk?

Accept	Defer	Mitigate
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑


System Problems
Threat Context
Step 15
History
How often has this threat occurred in the past?
How accurate are the data?
Very
Somewhat
Not At All
software defects
system crashes
hardware defects
malicious code
(virus, worm, Trojan horse, back door)
disclosure
modification
loss, destruction
interruption
_____ times in _____ years
❑

Threat Context	System Problems

Notes
What additional notes about each threat do you want to record?

Step 16

System Problems	Areas of Concern
Software Defects	
Give examples of how *software defects* could threaten this application.	
System Crashes	
Give examples of how *system crashes* could threaten this application.	
Hardware Defects	
Give examples of how *hardware defects* could threaten this application.	
Malicious Code	
Give examples of how *malicious code* could threaten this application. (Consider viruses, worms, Trojan horses, back doors, others)	

Areas of Concern

Software Defects
System Crashes
Hardware Defects
Malicious Code

6 Risk Profile Worksheet for Applications – Other Problems

	Phase 1 **Process S2** **Activity S2.3**
Step 12	Complete the threat tree for *other problems*. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on the threat tree, review the description and examples of that threat in the *Threat Translation Guide* (see pp. 72-77 of this workbook).
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.

continued

	Phase 3 **Process S4** **Activity S4.1**
Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) to each active threat.

	Phase 3 **Process S4** **Activity S4.3**
Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) to each active threat. Document your confidence level in your probability estimate.

	Phase 3 **Process S5** **Activity S5.2**
Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of the following worksheet.

Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.

Other Problems **Basic Risk Profile**

Step 12 **Step 22**

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Impact Values

What is the potential impact on the organization in each applicable area?

Asset	Actor	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other
	power supply problems	disclosure						
		modification						
		loss, destruction						
		interruption						
	telecommunications problems or unavailability	disclosure						
		modification						
		loss, destruction						
		interruption						
	third-party problems or unavailability of third-party systems	disclosure						
		modification						
		loss, destruction						
		interruption						
	natural disasters (e.g., flood, fire, tornado)	disclosure						
		modification						
		loss, destruction						
		interruption						

Basic Risk Profile | **Other Problems**

Step 24

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Step 26

Security Practice Areas

What is the stoplight status for each security practice area?

Step 27

Approach

What is your approach for addressing each risk?

Value	Confidence			Strategic						Operational									Approach		
	Very	Somewhat	Not At All	1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt	Accept	Defer	Mitigate
	|	-------- |	-------- |																❑	❑	❑
	|	-------- |	-------- |																❑	❑	❑
	|	-------- |	-------- |																❑	❑	❑
	|	-------- |	-------- |																❑	❑	❑
	|	-------- |	-------- |																❑	❑	❑
	|	-------- |	-------- |																❑	❑	❑
	|	-------- |	-------- |																❑	❑	❑
	|	-------- |	-------- |																❑	❑	❑
	|	-------- |	-------- |																❑	❑	❑
	|	-------- |	-------- |																❑	❑	❑
	|	-------- |	-------- |																❑	❑	❑
	|	-------- |	-------- |																❑	❑	❑
	|	-------- |	-------- |																❑	❑	❑
	|	-------- |	-------- |																❑	❑	❑
	|	-------- |	-------- |																❑	❑	❑
	|	-------- |	-------- |																❑	❑	❑

Other Problems **Threat Context**

Step 15

			History			
			How often has this threat occurred in the past?	*How accurate are the data?*		
				Very	**Somewhat**	**Not At All**
		disclosure	_____ times in _____ years	❑	❑	❑
	power supply	modification	_____ times in _____ years	❑	❑	❑
	problems	loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑
		disclosure	_____ times in _____ years	❑	❑	❑
	telecommunications	modification	_____ times in _____ years	❑	❑	❑
	problems or unavailability	loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑
		disclosure	_____ times in _____ years	❑	❑	❑
	third-party problems	modification	_____ times in _____ years	❑	❑	❑
	or unavailability of third-party systems	loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑
		disclosure	_____ times in _____ years	❑	❑	❑
	natural disasters	modification	_____ times in _____ years	❑	❑	❑
	(e.g., flood, fire, tornado)	loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑

Threat Context | **Other Problems**

Notes
What additional notes about each threat do you want to record?

Step 16

Other Problems	Areas of Concern
Power Supply Problems	
Give examples of how *power supply problems* could threaten this application.	
Telecommunications Problems	
Give examples of how *telecommunications problems* could threaten this application.	
Third-Party Problems	
Give examples of how *third-party problems* could threaten this application.	
Natural Disasters	
Give examples of how *natural disasters* could threaten this application.	

Areas of Concern

Power Supply Problems
Telecommunications Problems
Third-Party Problems
Natural Disasters

Other Problems (cont.) **Basic Risk Profile**

Step 12

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Step 22

Impact Values

What is the potential impact on the organization in each applicable area?

Asset	Actor	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other
	physical configuration or arrangement of buildings, offices, or equipment	disclosure						
		modification						
		loss, destruction						
		interruption						
		disclosure						
		modification						
		loss, destruction						
		interruption						
		disclosure						
		modification						
		loss, destruction						
		interruption						
		disclosure						
		modification						
		loss, destruction						
		interruption						

Basic Risk Profile | **Other Problems (cont.)**

Step 24

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value	Confidence: Very	Somewhat	Not At All

Step 26

Security Practice Areas

What is the stoplight status for each security practice area?

Strategic						Operational									
1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt

Step 27

Approach

What is your approach for addressing each risk?

Accept	Defer	Mitigate
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑

Other Problems (cont.) **Threat Context**

Step 15

		History			
		How often has this threat occurred in the past?	*How accurate are the data?*		
			Very	**Somewhat**	**Not At All**
	disclosure	_____ times in _____ years	❑	❑	❑
physical configuration	modification	_____ times in _____ years	❑	❑	❑
or arrangement of buildings, offices, or equipment	loss, destruction	_____ times in _____ years	❑	❑	❑
	interruption	_____ times in _____ years	❑	❑	❑
	disclosure	_____ times in _____ years	❑	❑	❑
	modification	_____ times in _____ years	❑	❑	❑
	loss, destruction	_____ times in _____ years	❑	❑	❑
	interruption	_____ times in _____ years	❑	❑	❑
	disclosure	_____ times in _____ years	❑	❑	❑
	modification	_____ times in _____ years	❑	❑	❑
	loss, destruction	_____ times in _____ years	❑	❑	❑
	interruption	_____ times in _____ years	❑	❑	❑
	disclosure	_____ times in _____ years	❑	❑	❑
	modification	_____ times in _____ years	❑	❑	❑
	loss, destruction	_____ times in _____ years	❑	❑	❑
	interruption	_____ times in _____ years	❑	❑	❑

Threat Context | **Other Problems (cont.)**

Notes
What additional notes about each threat do you want to record?

Step 16

Other Problems (cont.)	**Areas of Concern**
Physical Configuration Problems	
Give examples of how *physical configuration of buildings, offices, or equipment* could threaten this application.	
Give examples of how _____ could threaten this application.	
Give examples of how _____ could threaten this application.	
Give examples of how _____ could threaten this application.	

Areas of Concern

	Physical Configuration Problems

7 Network Access Paths Worksheet

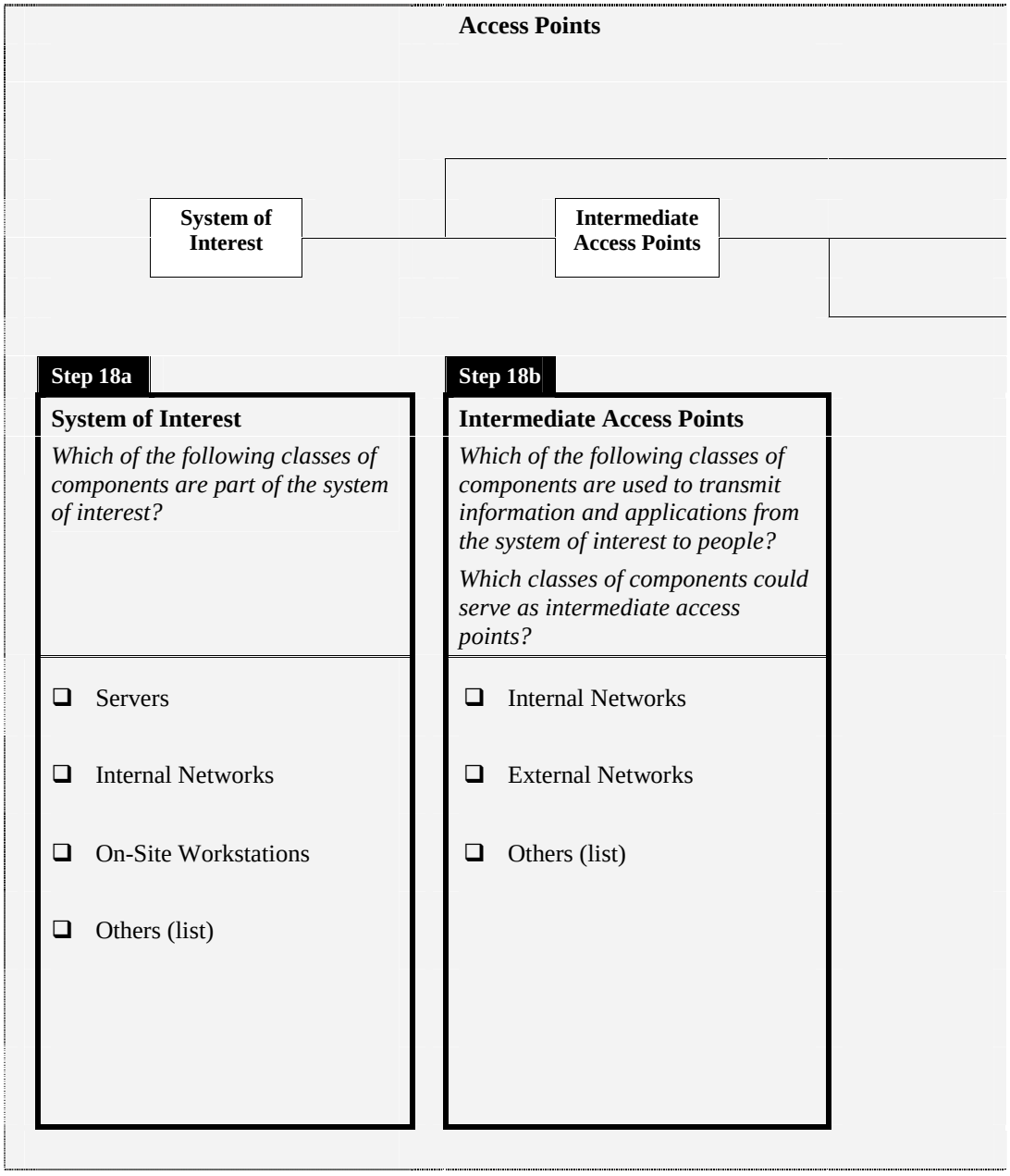
Phase 2
Process S3
Activity S3.1

Step 17	Select the system of interest for each critical asset (i.e., the system most closely related to the critical asset).
Step 18a	Review paths used to access each critical asset, and select key classes of components related to each critical asset. Determine which classes of components are part of the system of interest.
Step 18b	Determine which classes of components serve as intermediate access points (i.e., which components are used to transmit information and applications from the system of interest to people).
Step 18c	Determine which classes of components, both internal and external to the organization's networks, are used by people (e.g., users, attackers) to access the system.
Step 18d	Determine where information from the system of interest is stored for backup purposes.
Step 18e	Determine which other systems access information or applications from the system of interest and which other classes of components can be used to access critical information or services from the system of interest.

Step 17

System of Interest

What system or systems are most closely related to the critical asset?



Step 18a

System of Interest

Which of the following classes of components are part of the system of interest?

- ❑ Servers
- ❑ Internal Networks
- ❑ On-Site Workstations
- ❑ Others (list)

Step 18b

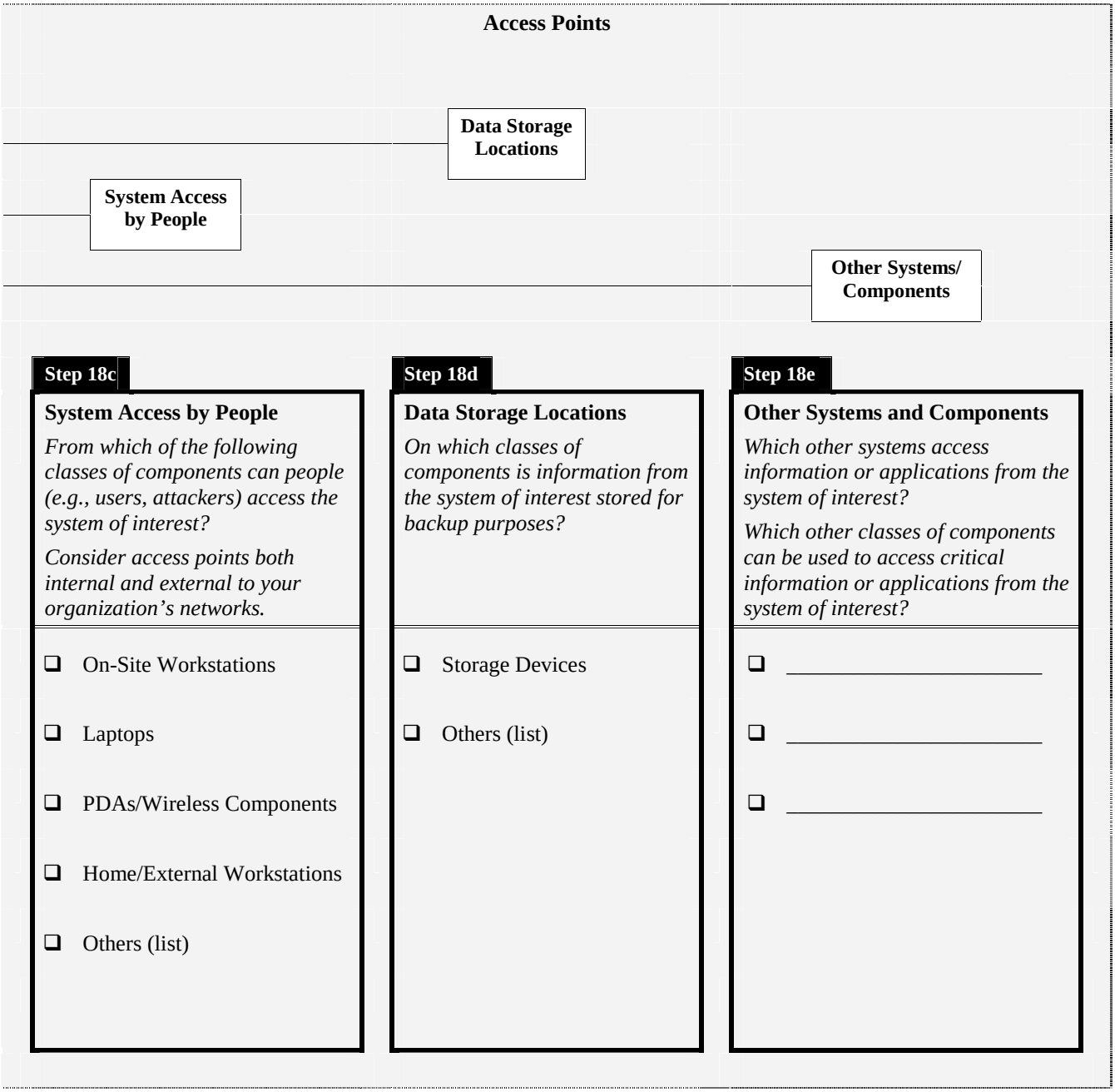
Intermediate Access Points

Which of the following classes of components are used to transmit information and applications from the system of interest to people?

Which classes of components could serve as intermediate access points?

- ❑ Internal Networks
- ❑ External Networks
- ❑ Others (list)

***Note**: When you select a key class of components, make sure that you also document any relevant subclasses or specific examples when appropriate.*



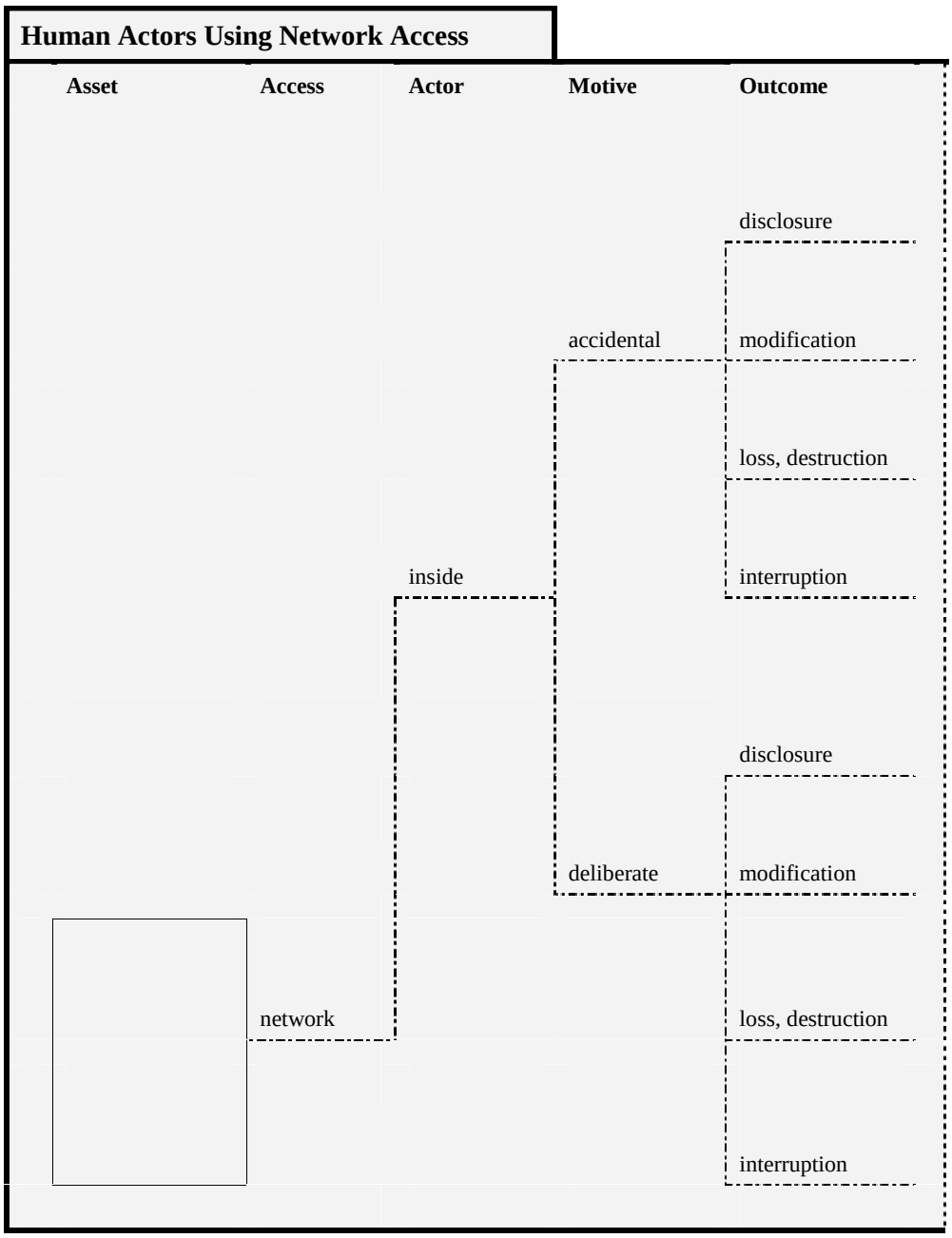
8 Threat Translation Guide

Phase 1
Process S2
Activity S2.3

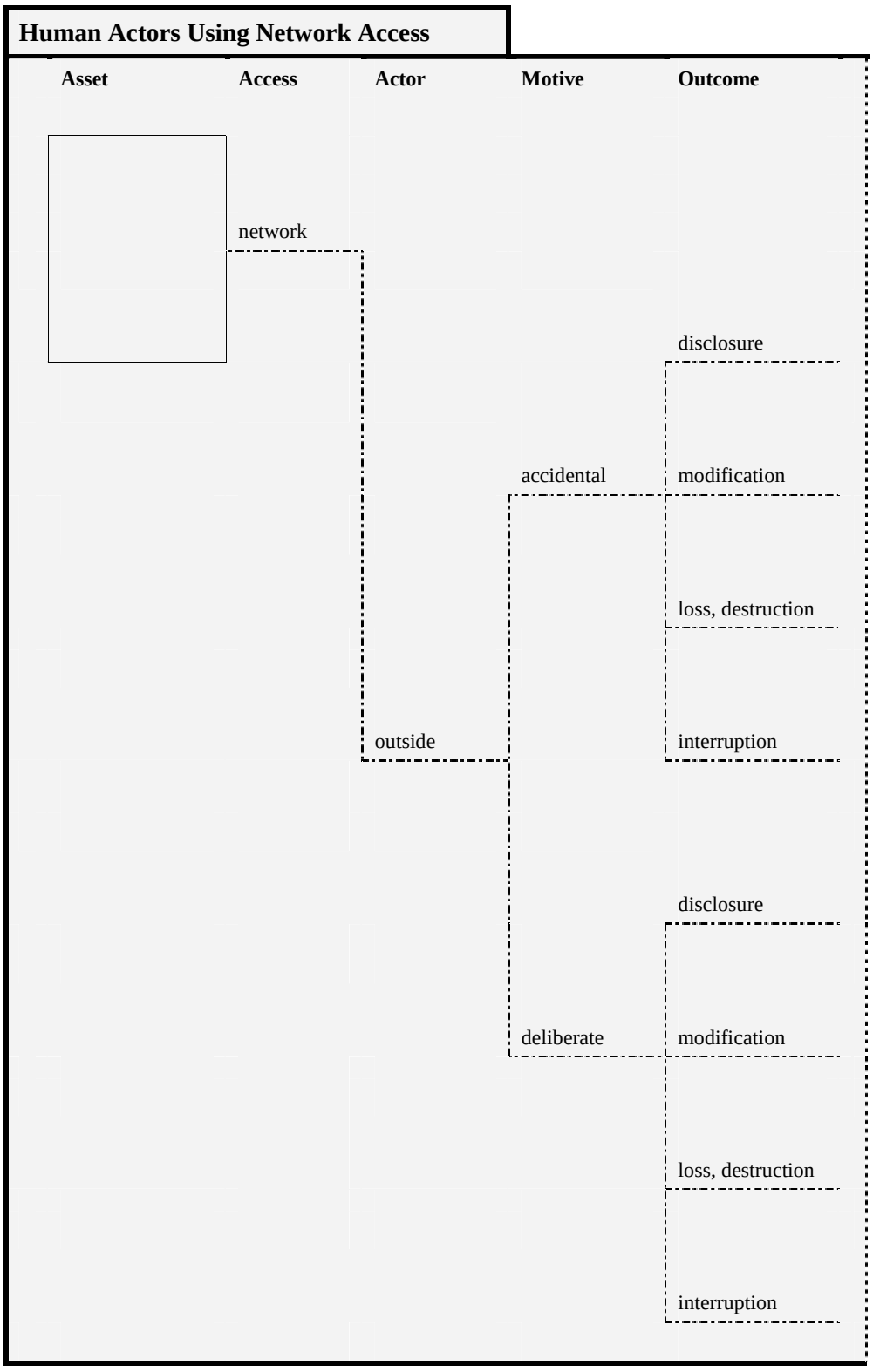
Threat Translation Guide

The *Threat Translation Guide* describes each branch of an asset-based threat tree. If you have difficulty understanding the types of threats represented by a branch, you can use this guide to decipher the meaning of that branch.

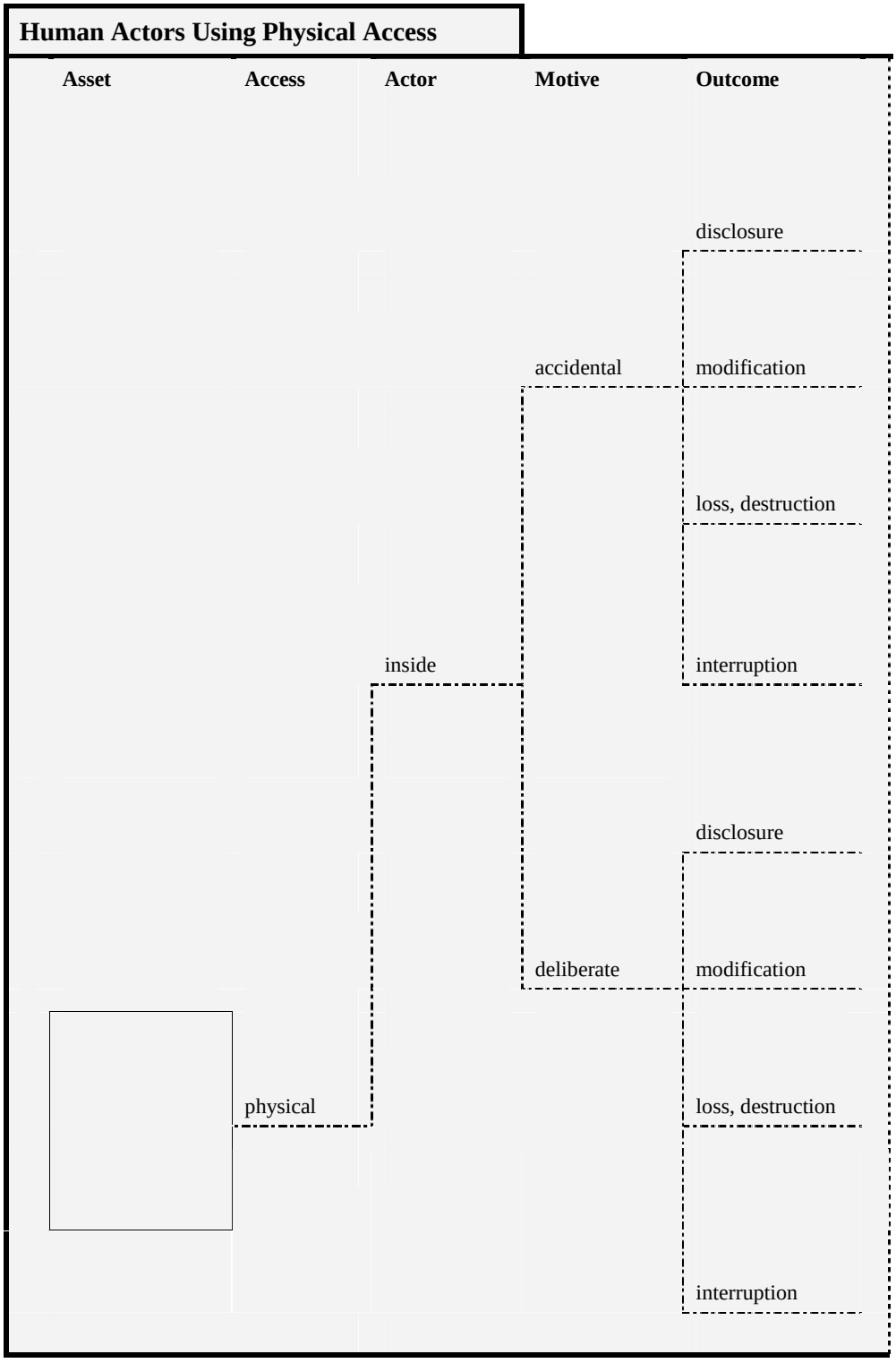
You will find asset-based threat trees for the following sources of threat:


Human Actors Using Network Access
Asset
Access
Actor
Motive
Outcome
disclosure
accidental
modification
loss, destruction
inside
interruption
disclosure
deliberate
modification
network
loss, destruction
interruption

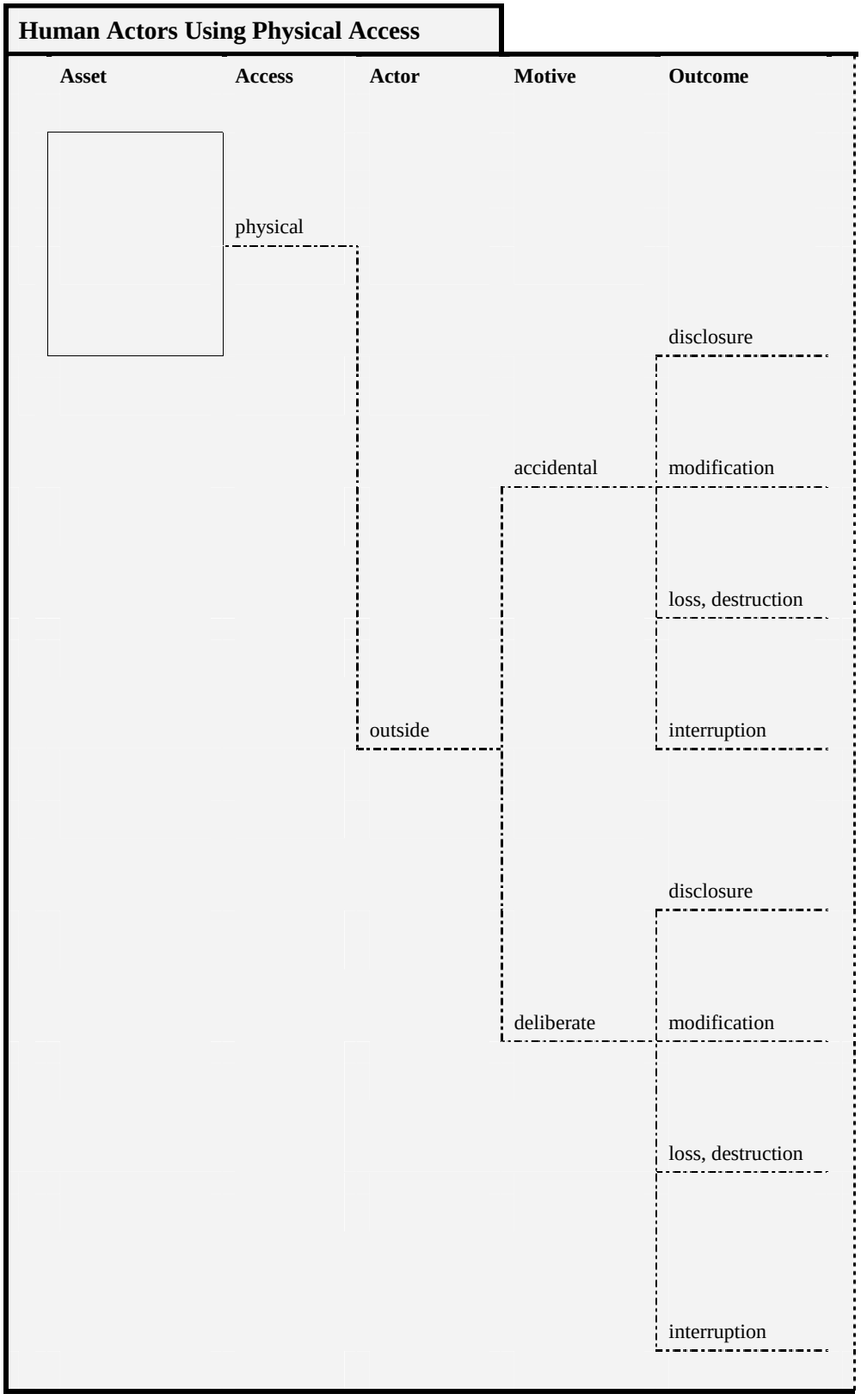
Description	Example
A staff member without malicious intent who has legitimate access to the computing infrastructure accidentally views confidential information on an important system.	Incorrect file permissions enable a staff member to accidentally access a restricted personnel database.
A staff member without malicious intent who has legitimate access to the computing infrastructure accidentally modifies information on an important system.	A staff member accidentally enters incorrect financial data into a customer database.
A staff member without malicious intent who has legitimate access to the computing infrastructure accidentally loses or destroys information on an important system.	A staff member deletes an important customer file by mistake.
A staff member without malicious intent who has legitimate access to the computing infrastructure accidentally interrupts access to an important system.	A staff member who is not computer savvy inadvertently crashes an important system.
A staff member with malicious intent who has legitimate access to the computing infrastructure exploits that access to deliberately view confidential information on an important system.	A staff member uses access to a restricted personnel database to deliberately view information in that database that is restricted by policy.
A staff member with malicious intent who has legitimate access to the computing infrastructure exploits that access to deliberately modify information on an important system.	A staff member responsible for data entry deliberately enters incorrect customer information into a database.
A staff member with malicious intent who has legitimate access to the computing infrastructure exploits that access to deliberately lose or destroy information on an important system.	A staff member with access to design documents for a new product deliberately deletes the files that contain those design documents.
A staff member with malicious intent who has legitimate access to the computing infrastructure exploits that access to deliberately interrupt access to an important system.	A staff member uses legitimate access to the computing infrastructure to launch a denial-of-service attack on an important system.


Human Actors Using Network Access
Asset
Access
Actor
Motive
Outcome
network
outside
accidental
deliberate
disclosure
modification
loss, destruction
interruption
disclosure
modification
loss, destruction
interruption

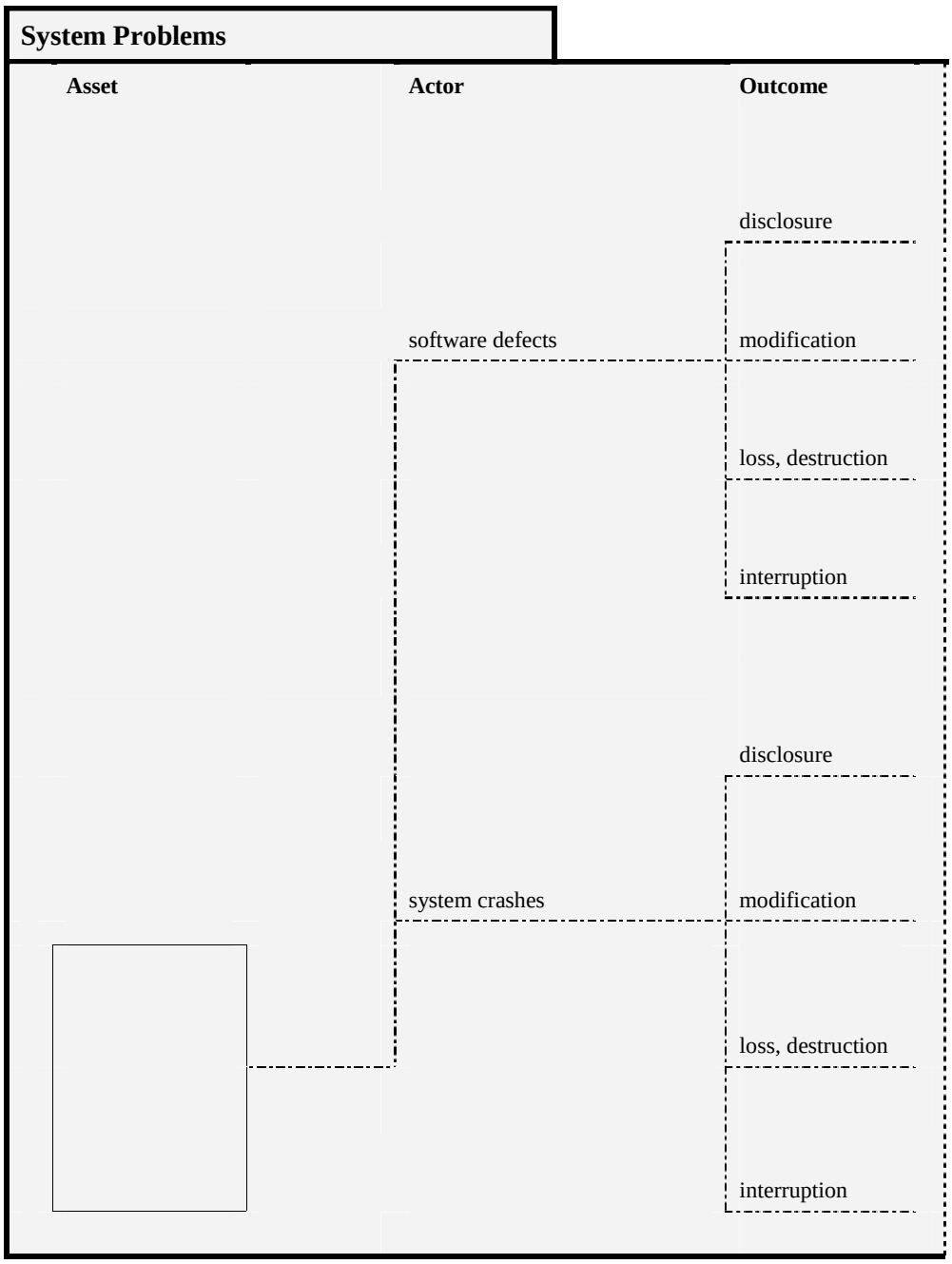
Description	Example
An outsider without malicious intent gains access to your computing infrastructure (legitimately or by accident) and views confidential data on a system.	Temporary employees are given access to your computing infrastructure to help with an increased workload. While performing their job duties, one of them accidentally views confidential personnel data.
An outsider without malicious intent gains access to your computing infrastructure (legitimately or by accident) and accidentally modifies information on a system.	Temporary employees are given access to your computing infrastructure to help with an increased workload. While performing their job duties, one of them accidentally modifies important customer data.
An outsider without malicious intent gains access to your computing infrastructure (legitimately or by accident) and loses or destroys information on a system.	Temporary employees are given access to your computing infrastructure to help with an increased workload. While performing their job duties, one of them accidentally loses or destroys financial data.
An outsider without malicious intent gains access to your computing infrastructure (legitimately or by accident) and accidentally interrupts access to a system.	Temporary employees are given access to your computing infrastructure to help with an increased workload. While performing their job duties, one of them accidentally crashes an important system.
An attacker with malicious intent deliberately exploits vulnerabilities in the computing infrastructure to view confidential information.	A corporate spy exploits vulnerabilities in the computing infrastructure to gain unauthorized access to a key business system. The spy uses that access to view confidential customer information on the system.
An attacker with malicious intent deliberately exploits vulnerabilities in the computing infrastructure to modify information.	A corporate spy exploits vulnerabilities in the computing infrastructure to gain unauthorized access to a key business system. The spy uses that access to modify financial data on the system.
An attacker with malicious intent deliberately exploits vulnerabilities in the computing infrastructure to lose or destroy information.	A corporate spy exploits vulnerabilities in the computing infrastructure to gain unauthorized access to a key business system. The spy uses that access to lose or destroy a new product design on the system.
An attacker with malicious intent deliberately exploits vulnerabilities in the computing infrastructure to interrupt access to a system.	A corporate spy exploits vulnerabilities in the computing infrastructure to gain unauthorized access to an airline's scheduling system. The spy uses that access to crash the system and prevent real-time updates.


Human Actors Using Physical Access
Asset
Access
Actor
Motive
Outcome
disclosure
accidental
modification
loss, destruction
inside
interruption
disclosure
deliberate
modification
physical
loss, destruction
interruption

Description	Example
A staff member without malicious intent accidentally views confidential information after gaining physical access to a system, one of its components, or a physical copy of the information.	A staff member accidentally sees confidential information on (1) a colleague's computer screen or (2) a printout on a colleague's desk.
A staff member without malicious intent accidentally modifies information after gaining physical access to a system, one of its components, or a physical copy of the information.	A staff member modifies information by (1) accidentally altering information on a colleague's computer while using it for another purpose or (2) accidentally taking a page of a printout on a colleague's desk.
A staff member without malicious intent accidentally loses or destroys information after gaining physical access to a system, one of its components, or a physical copy of the information.	A staff member loses or destroys information by (1) accidentally deleting information from a colleague's computer while using it or (2) shredding a paper accidentally taken from a colleague's desk.
A staff member without malicious intent interrupts access to a system or information by accidentally using physical access to a system, one of its components, or a physical copy of the information to prevent others from accessing the system or information.	A staff member interrupts access to a system by (1) accidentally crashing the system while accessing it from a colleague's computer or (2) locking the keys inside an office where a physical file is stored.
A staff member with malicious intent deliberately views confidential information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A staff member uses unauthorized access to a physically restricted area of the building to deliberately (1) view confidential information on a computer or (2) read a confidential memo lying on a desk.
A staff member with malicious intent deliberately modifies information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A staff member uses unauthorized access to a physically restricted area of the building to deliberately (1) modify information on a computer or (2) modify a physical file lying on a desk.
A staff member with malicious intent deliberately loses or destroys information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A staff member uses unauthorized access to a physically restricted area of the building to deliberately (1) delete information on a computer or (2) destroy a physical file lying on a desk.
A staff member with malicious intent deliberately interrupts access to an important system or information by breeching physical security to a system, one of its components, or a physical copy of the information and using that physical access to prevent others from accessing the system or information.	A staff member uses unauthorized access to a physically restricted area of the building to (1) gain access to and then deliberately crash an important business system or (2) jam the door and prevent others from physically accessing the systems and information located in that area of the building.

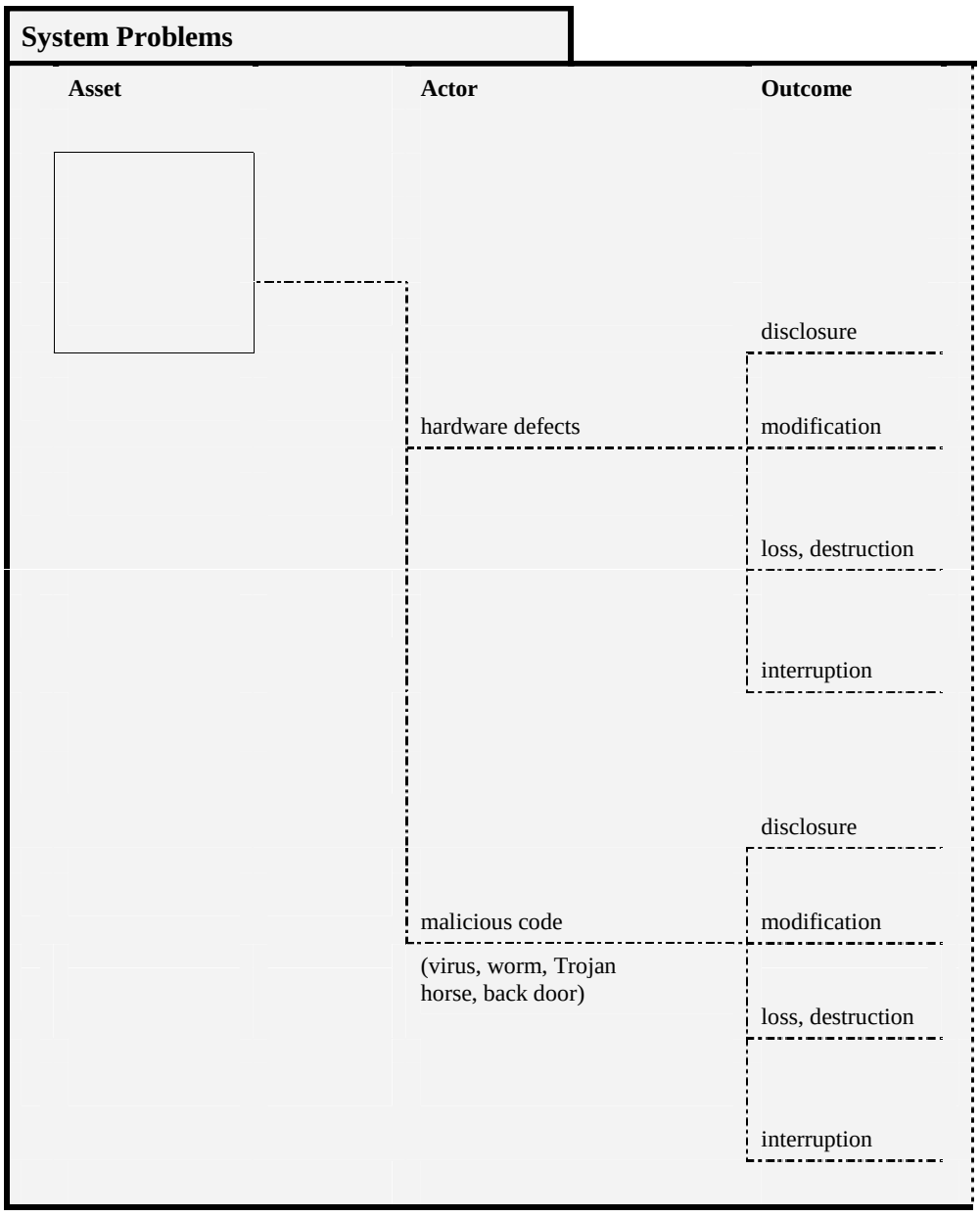

Human Actors Using Physical Access
Asset
Access
Actor
Motive
Outcome
physical
disclosure
accidental
modification
loss, destruction
outside
interruption
disclosure
deliberate
modification
loss, destruction
interruption

Description	Example
An outsider without malicious intent gains physical access to your computing infrastructure or a physical copy of information and uses that access to view confidential information accidentally.	A consultant is given access to a staff member's office and accidentally sees confidential information on (1) a staff member's computer screen or (2) a printout on a staff member's desk.
An outsider without malicious intent gains physical access to your computing infrastructure or a physical copy of information and uses that access to modify information accidentally.	A consultant is given access to the computer room and (1) accidentally makes the wrong change to a configuration file on a server or (2) accidentally records the wrong information in a maintenance log.
An outsider without malicious intent gains physical access to your computing infrastructure or a physical copy of information and uses that access to lose or destroy information accidentally.	A consultant configuring one of your servers is given access to the computer room and accidentally (1) destroys an important electronic file or (2) throws away an important piece of system documentation.
An outsider without malicious intent gains physical access to your computing infrastructure or a physical copy of information and uses that access to accidentally prevent others from accessing the information.	A consultant configuring one of your servers is given access to the computer room and accidentally (1) crashes a system while accessing it or (2) locks the keys to the computer room inside it after he or she leaves.
An attacker with malicious intent deliberately views confidential information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A corporate spy poses as a member of the cleaning crew to gain unauthorized physical access to a competitor's site and view confidential information either (1) on a key business system or (2) in a physical file.
An attacker with malicious intent deliberately modifies information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A corporate spy poses as a member of the cleaning crew to gain unauthorized physical access to a competitor's site and modify financial information either (1) on a key business system or (2) in a physical file.
An attacker with malicious intent deliberately loses or destroys information by breeching physical security and accessing components of the computing infrastructure or a physical copy of the information.	A corporate spy poses as a member of the cleaning crew to gain unauthorized physical access to a competitor's site and destroy customer information either (1) on a key business system or (2) in a physical file.
An attacker with malicious intent deliberately interrupts access to an important system or information by breeching physical security to a system, one of its components, or a physical copy of the information and by using that physical access to prevent others from accessing the system or information.	A corporate spy poses as a member of the cleaning crew to gain unauthorized physical access to a competitor's site and (1) deliberately crashes an important business system or (2) jams the door to prevent others from physically accessing the systems and information located in an area of the building.



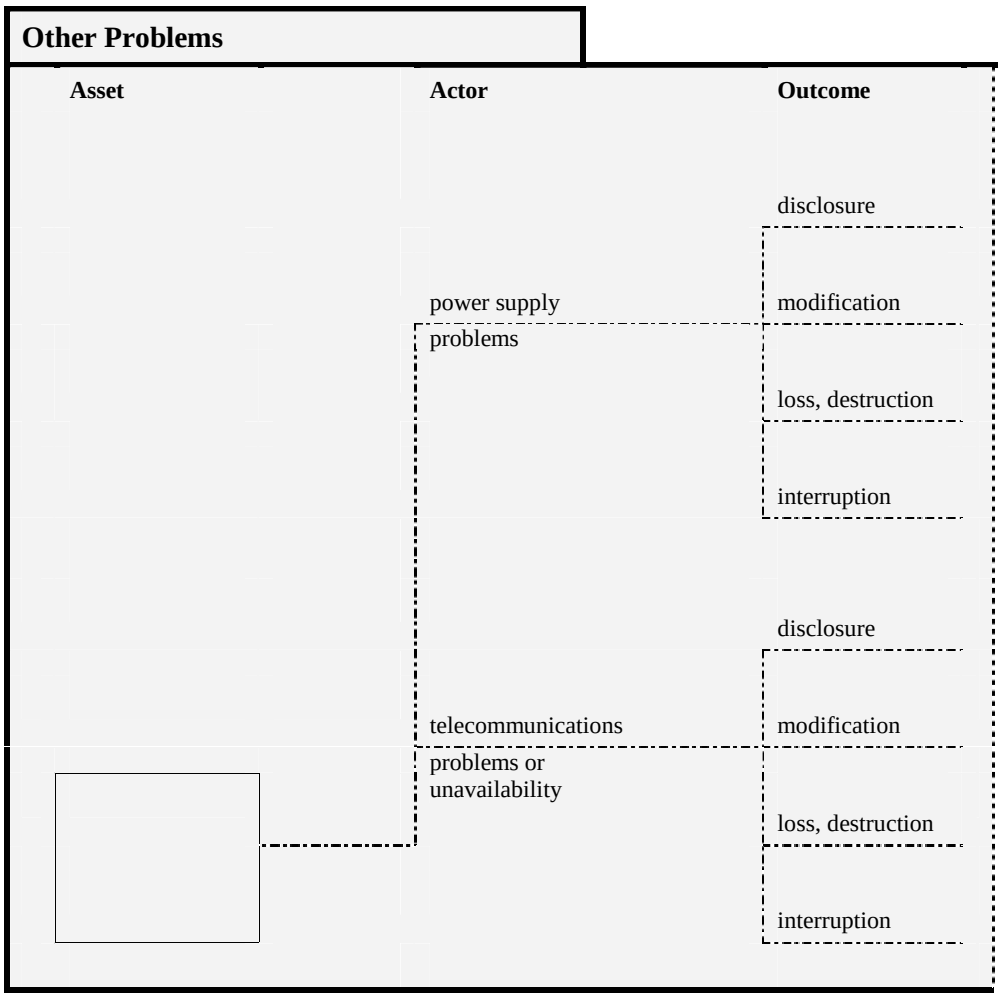
* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
A software defect results in disclosure of information to unauthorized parties.	A defect in a computer's operating system changes file access permissions to permit world read and write permissions on certain files and directories.
A software defect results in modification of information on a system.	A custom software application incorrectly performs mathematical operations on data, affecting the integrity of the results.
A software defect results in the loss or destruction of information on a system.	A word processing application is known to crash computers periodically because of a problem with a specific command sequence, destroying any information that was not saved.
A software defect results in a system crash, preventing access to the system.	A word processing application is known to crash computers periodically because of a problem with a specific command sequence, preventing access to that computer.
A system crashes for unknown reasons (i.e., it cannot be traced to a software defect, hardware defect, malicious code, or actions by people), resulting in disclosure of information to unauthorized parties.	---
A system crashes for unknown reasons (i.e., it cannot be traced to a software defect, hardware defect, malicious code, or actions by people), resulting in modification of information on that system.	A system crashes during a lengthy update of a financial database, corrupting the information in the database.
A system crashes for unknown reasons (i.e., it cannot be traced to a software defect, hardware defect, malicious code, or actions by people), resulting in the loss or destruction of information on that system.	A customer database system frequently crashes, destroying any information that was not saved at the time of the crash.
A system crashes for unknown reasons (i.e., it cannot be traced to a software defect, hardware defect, malicious code, or actions by people), resulting in interruption of access to that system.	An email server crashes, resulting in interruption of user access to email.



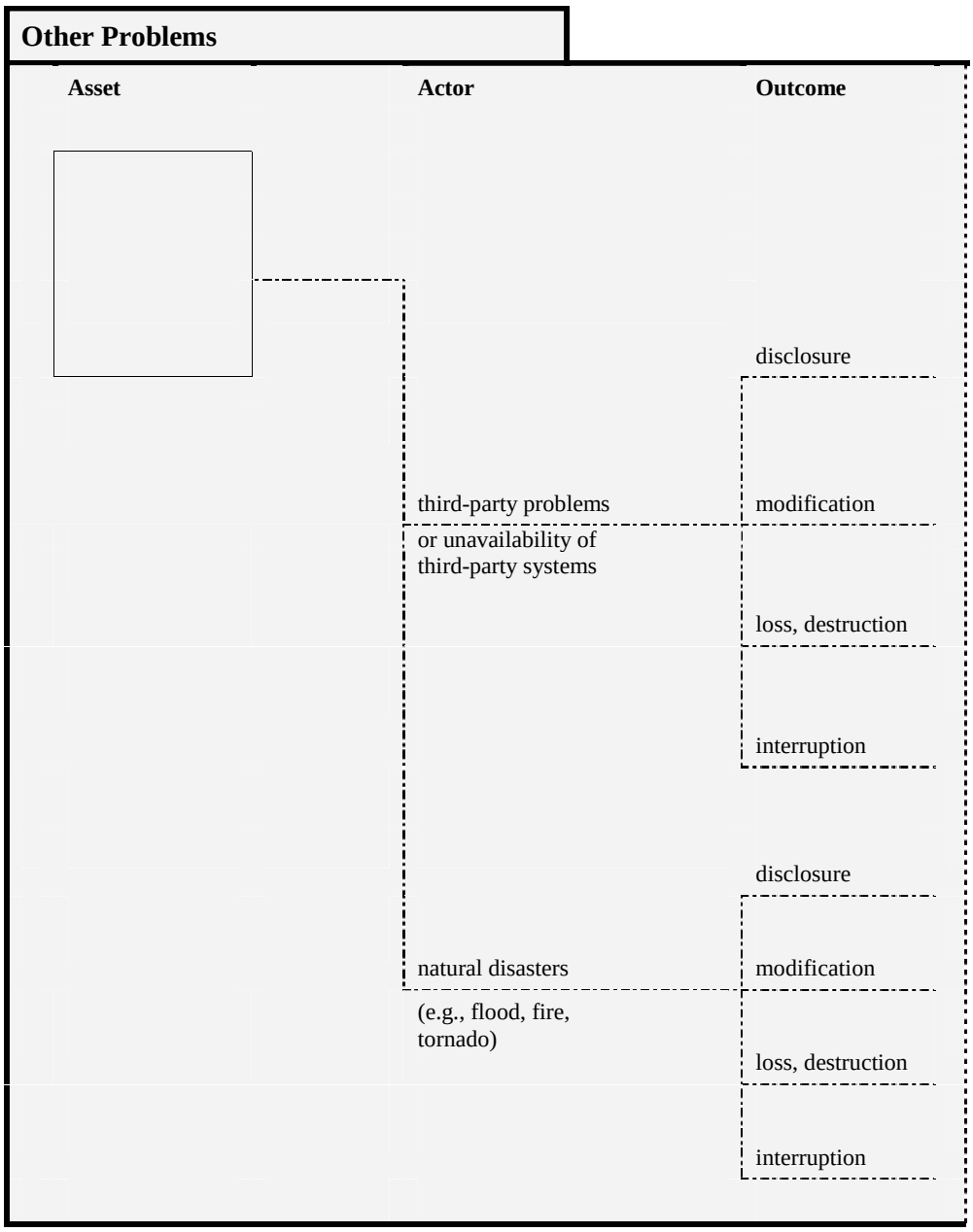
* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
A hardware defect results in disclosure of information to unauthorized parties.	---
A hardware defect results in modification of information on a system.	A disk drive develops a hardware problem that affects the integrity of a database that is stored on the disk.
A hardware defect results in the loss or destruction of information on a system.	A disk drive develops a hardware problem that ends up destroying the information on the disk. Files can be retrieved only from backups.
A hardware defect results in a system crash, preventing access to the system.	A disk drive develops a hardware problem, preventing access to any information on the disk until the problem is corrected.
A system is affected by malicious code (virus, worm, Trojan horse, back door) that enables unauthorized parties to view information.	A back door on a system enables unauthorized people to access the system and view customer credit card information on that system.
A system is affected by malicious code (virus, worm, Trojan horse, back door) that modifies information on that system.	A system is infected with a virus that modifies a process control application on the computer's disk drive.
A system is affected by malicious code (virus, worm, Trojan horse, back door) that deletes information on that system.	A system is infected with a virus that deletes all information on the computer's disk drive.
A system is affected by malicious code (virus, worm, Trojan horse, back door) that results in the system crashing.	A system is infected with a virus that is spread via email, slowing network traffic and creating a denial-of-services attack.



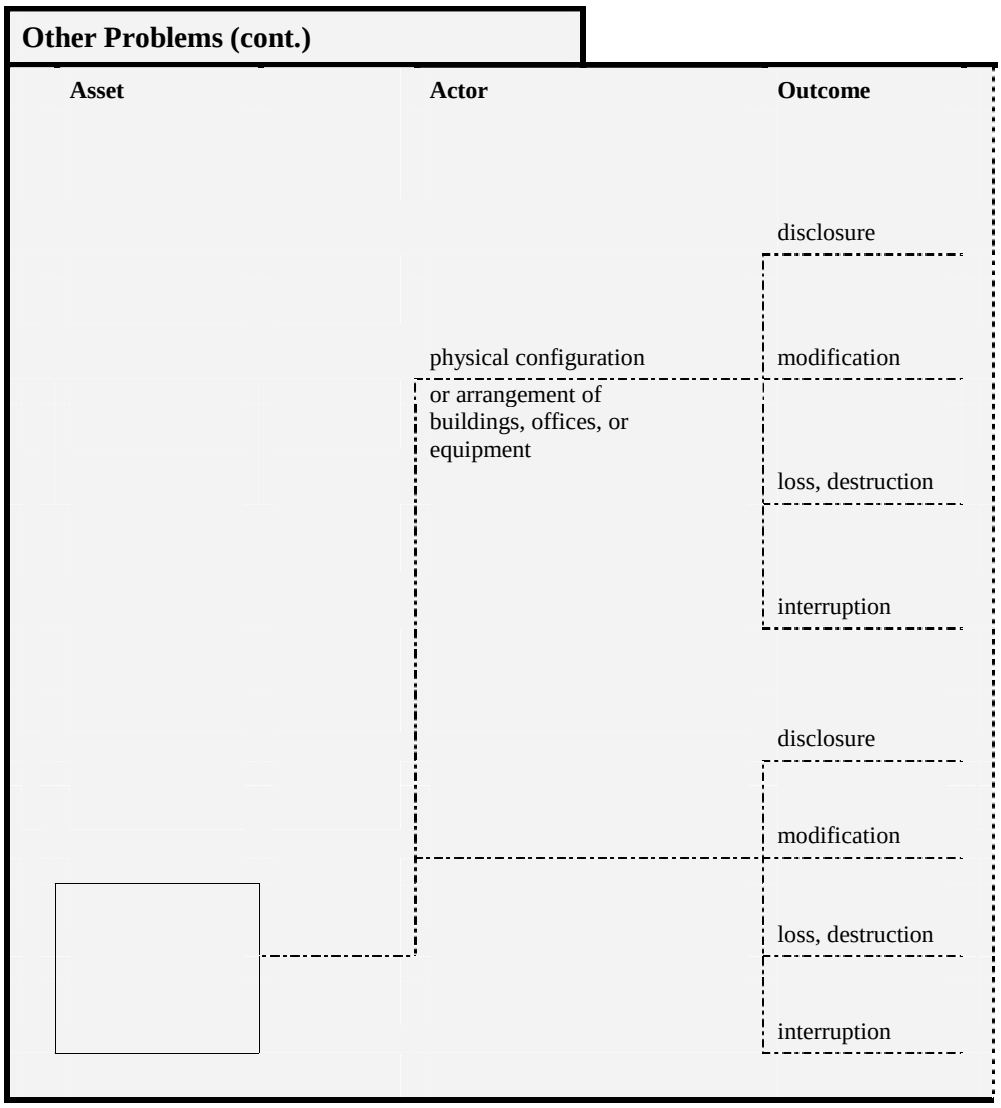
* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
Problems with the power supply lead to disclosure of information to unauthorized parties.	---
Problems with the power supply lead to modification of information on a system.	---
Problems with the power supply lead to loss or destruction of information on a system.	A power outage results in loss of any information that was not saved at the time of the outage.
Problems with the power supply lead to interruption of access to a system.	A power outage prevents access to all key business systems.
Unavailability of telecommunications services leads to disclosure of information to unauthorized parties.	---
Unavailability of telecommunications services leads to modification of information on a system.	---
Unavailability of telecommunications services leads to loss or destruction of information on a system.	---
Unavailability of telecommunications services leads to interruption of access to a system.	The unavailability of the telecommunications link prevents access to a key business system located at a remote site.



* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
Problems with services provided by third parties (e.g., maintenance of systems) lead to disclosure of information to unauthorized parties.	A staff member from a third-party service provider views confidential information on a key business system that is maintained by that service provider.
Problems with services provided by third parties (e.g., maintenance of systems) lead to modification of information on a system.	Problems at a third-party service provider lead to the modification of information on a key business system located at that provider's site and maintained by the provider.
Problems with services provided by third parties (e.g., maintenance of systems) lead to loss or destruction of information on a system.	Problems at a third-party service provider lead to the destruction of information on a key business system located at that provider's site and maintained by the provider.
Problems with services provided by third parties (e.g., maintenance of systems) lead to interruption of access to a system.	A system maintained by a third-party service provider and located at the provider's site is unavailable due to problems created by that provider's staff.
Natural disasters (e.g., flood, fire, tornado) lead to disclosure of information to unauthorized parties.	People at the site of a tornado see confidential memos that are dispersed among the debris.
Natural disasters (e.g., flood, fire, tornado) lead to modification of information.	---
Natural disasters (e.g., flood, fire, tornado) lead to loss or destruction of information.	The flooding of a basement area destroys paper records that are stored there.
Natural disasters (e.g., flood, fire, tornado) lead to interruption of access to a system.	The flooding of a computer room in the basement of a building prevents access to systems in that room.



* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
The physical configuration or arrangement of buildings, offices, or equipment leads to disclosure of information to unauthorized parties.	The layout of an office workspace enables anyone in the area to view customer credit card information displayed on computer screens.
The physical configuration or arrangement of buildings, offices, or equipment leads to modification of information on a system.	---
The physical configuration or arrangement of buildings, offices, or equipment leads to loss or destruction of information on a system.	---
The physical configuration or arrangement of buildings, offices, or equipment leads to interruption of access to a system.	---

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
OCTAVE-S Implementation Guide, Version 1.0, Volume 7	F19628-00-C-0003

6. AUTHOR(S)

Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody

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

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

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

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

14. SUBJECT TERMS	15. NUMBER OF PAGES
information security, risk management, OCTAVE	78

16. PRICE CODE

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

OCTAVE®-S Implementation Guide, Version 1.0

Volume 8: Critical Asset Worksheets for People

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

HANDBOOK
CMU/SEI-2003-HB-003

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

OCTAVE®-S Implementation Guide, Version 1.0

Volume 8: Critical Asset Worksheets for People

CMU/SEI-2003-HB-003

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

Networked Systems Survivability Program

This report was prepared for the

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

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

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

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

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

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

Table of Contents

List of Tables

About This Document

This document is Volume 6 of the *OCTAVE-S Implementation Guide*, a 10-volume handbook supporting the OCTAVE-S methodology. This volume provides worksheets to document data related to critical assets that are categorized as people.

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℠ (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 Introduction

This document contains the Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE®)-S worksheets related to critical assets that are people. The activities related to these worksheets are focused on analyzing a critical asset.

Table 1 provides a brief introduction to the contents of this workbook, using activity step numbers as a key. For more details about how to complete each step, refer to the *OCTAVE®-S Method Guidelines*, which can be found in Volume 3 of the *OCTAVE®-S Implementation Guide*.

Table 1: Worksheets Provided in This Workbook

Step	Description	Worksheet	Activity	Pages
Step 6	Start a *Critical Asset Information worksheet* for each critical asset. Record the name of the critical asset on its *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 7	Record your rationale for selecting each critical asset on that asset's *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 8	Record a description for each critical asset on that asset's *Critical Asset Selection worksheet*. Consider who uses each critical asset as well as who is responsible for it.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 9	Record assets that are related to each critical asset on that asset's *Critical Asset Information worksheet*. Refer to the *Asset Identification worksheet* to determine which assets are related to each critical asset.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8

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

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

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 10	Record the security requirements for each critical asset on that asset's *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 11	For each critical asset, record the most important security requirement on that asset's *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 12	Complete all appropriate threat trees for each critical asset. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on any threat tree, review the description and examples of that threat in the *Threat Translation Guide*.	Risk Profile Threat Translation Guide	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-24
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.	Risk Profile	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-24
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.	Risk Profile	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-24
Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) for each active threat to each critical asset.	Risk Profile Impact Evaluation Criteria	Phase 3 Process S4 S4.1 Evaluate Impacts of Threats	9-24
Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) for each active threat to each critical asset. Document your confidence level in your probability estimate.	Risk Profile Probability Evaluation Criteria	Phase 3 Process S4 S4.3 Evaluate Probabilities of Threats	9-24

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of each critical asset's *Risk Profile worksheet*.	Risk Profile Security Practices	Phase 3 Process S5 S5.2 Select Mitigation Approaches	9-24
Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.	Risk Profile	Phase 3 Process S5 S5.2 Select Mitigation Approaches	9-24

2 Critical Asset Information Worksheet for People

	Phase 1 **Process S2** **Activity S2.1**
Step 6	Start a *Critical Asset Information worksheet* for each critical asset. Record the name of the critical asset on its *Critical Asset Information worksheet*.
Step 7	Record your rationale for selecting each critical asset on that asset's *Critical Asset Information worksheet*.
Step 8	Record a description for each critical asset on that asset's *Critical Asset Selection worksheet*. Consider who uses each critical asset as well as who is responsible for it.
Step 9	Record assets that are related to each critical asset on that asset's *Critical Asset Information worksheet*. Refer to the *Asset Identification worksheet* to determine which assets are related to each critical asset.
	Phase 1 **Process S2** **Activity S2.2**
Step 10	Record the security requirements for each critical asset on that asset's *Critical Asset Information worksheet*.
Step 11	For each critical asset, record the most important security requirement on that asset's *Critical Asset Information worksheet*.

Step 6	Step 7
Critical Asset	**Rationale for Selection**
What is the critical person(s)?	*Why is this person(s) critical to the organization?*

Step 9	
Related Assets	
Which assets are related to this person(s)?	
Systems:	Information:
Applications:	Other:

Step 8

Description
What special skills or knowledge are provided by this person(s)?

Step 10

Security Requirements		**Step 11** **Most Important Security Requirement**
What are the security requirements for this person(s)? *(Hint: Focus on what the security requirements should be, not what they currently are.)*		*Which security requirement is most important for this person(s)?*
❑ Availability	The set of skills provided by_____ must be available when needed.	❑ Availability ❑ Other
❑ Other	_____ _____	

3 Risk Profile Worksheet for People – Other Problems

Phase 1
Process S2
Activity S2.3

Step 12	Complete the threat tree for *other problems*. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on the threat tree, review the description and examples of that threat in the *Threat Translation Guide* (see pp. 26-30 of this workbook).
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.

continued

	Phase 3 **Process S4** **Activity S4.1**
Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) to each active threat.

	Phase 3 **Process S4** **Activity S4.3**
Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) to each active threat. Document your confidence level in your probability estimate.

	Phase 3 **Process S5** **Activity S5.2**
Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of the following worksheet.

Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.

Other Problems | **Basic Risk Profile**

Step 12

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Step 22

Impact Values

What is the potential impact on the organization in each applicable area?

Asset	Actor	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other
	key people taking a temporary leave of absence (e.g., due to illness, disability)	disclosure						
		modification						
		loss, destruction						
		interruption						
	key people leaving the organization permanently (e.g., retirement, other opportunities)	disclosure						
		modification						
		loss, destruction						
		interruption						
	threats affecting a third-party or service provider	disclosure						
		modification						
		loss, destruction						
		interruption						
		disclosure						
		modification						
		loss, destruction						
		interruption						

Basic Risk Profile | **Other Problems**

Step 24 | **Step 26** | **Step 27**

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value **Confidence**

	Very	Somewhat	Not At All

Security Practice Areas

What is the stoplight status for each security practice area?

	Strategic						Operational								
	1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt
		■		■	■		■	■	■	■	■	■	■	■	■
		■		■	■		■	■	■	■	■	■	■	■	■
		■		■	■		■	■	■	■	■	■	■	■	■
		■		■	■		■	■	■	■	■	■	■	■	■
		■		■	■		■	■	■	■	■	■	■	■	■
		■		■	■		■	■	■	■	■	■	■	■	■
		■		■	■		■	■	■	■	■	■	■	■	■
		■		■	■		■	■	■	■	■	■	■	■	■
		■		■			■	■	■	■	■	■	■	■	■
		■		■			■	■	■	■	■	■	■	■	■
		■		■			■	■	■	■	■	■	■	■	■
		■		■			■	■	■	■	■	■	■	■	■

Approach

What is your approach for addressing each risk?

Accept	Defer	Mitigate
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑

Other Problems

Threat Context

Step 15

			History			
			How often has this threat occurred in the past?	*How accurate are the data?*		
				Very	**Somewhat**	**Not At All**
key people taking a temporary leave of absence (e.g., due to illness, disability)		disclosure	_____ times in _____ years	❑	❑	❑
		modification	_____ times in _____ years	❑	❑	❑
		loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑
key people leaving the organization permanently (e.g., retirement, other opportunities)		disclosure	_____ times in _____ years	❑	❑	❑
		modification	_____ times in _____ years	❑	❑	❑
		loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑
threats affecting a third-party or service provider		disclosure	_____ times in _____ years	❑	❑	❑
		modification	_____ times in _____ years	❑	❑	❑
		loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑
		disclosure	_____ times in _____ years	❑	❑	❑
		modification	_____ times in _____ years	❑	❑	❑
		loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑

Threat Context	Other Problems

Notes
What additional notes about each threat do you want to record?

Step 16

Other Problems	Areas of Concern
People Taking a Temporary Leave of Absence	
Give examples of how *key people taking a temporary leave of absence* could affect the ability of this person or group of people to provide critical services, skills, and knowledge.	
People Leaving the Organization Permanently	
Give examples of how *key people leaving the organization permanently* could affect the ability of this person or group of people to provide critical services, skills, and knowledge.	
Threats Affecting a Third-Party	
Give examples of how *threats affecting a third party or service provider* could affect the ability of that third-party or service provider to provide critical services, skills, and knowledge.	
Give examples of how _____ could affect the ability of this person or group of people to provide critical services, skills, and knowledge.	

Areas of Concern

People Taking a Temporary Leave of Absence
People Leaving the Organization Permanently
Threats Affecting a Third-Party

Other Problems (cont.) **Basic Risk Profile**

Step 12

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Step 22

Impact Values

What is the potential impact on the organization in each applicable area?

Asset	Actor	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other
		disclosure						
		modification						
		loss, destruction						
		interruption						
		disclosure						
		modification						
		loss, destruction						
		interruption						
		disclosure						
		modification						
		loss, destruction						
		interruption						
		disclosure						
		modification						
		loss, destruction						
		interruption						

Basic Risk Profile | **Other Problems (cont.)**

Step 24

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value	Confidence: Very	Somewhat	Not At All

Step 26

Security Practice Areas

What is the stoplight status for each security practice area?

Strategic						Operational								
1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt

Step 27

Approach

What is your approach for addressing each risk?

Accept	Defer	Mitigate
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑

Other Problems (cont.)

Threat Context

Step 15

		History			
		How often has this threat occurred in the past?	*How accurate are the data?*		
			Very	**Somewhat**	**Not At All**
	disclosure	_____ times in _____ years	❑	❑	❑
	modification	_____ times in _____ years	❑	❑	❑
	loss, destruction	_____ times in _____ years	❑	❑	❑
	interruption	_____ times in _____ years	❑	❑	❑
	disclosure	_____ times in _____ years	❑	❑	❑
	modification	_____ times in _____ years	❑	❑	❑
	loss, destruction	_____ times in _____ years	❑	❑	❑
	interruption	_____ times in _____ years	❑	❑	❑
	disclosure	_____ times in _____ years	❑	❑	❑
	modification	_____ times in _____ years	❑	❑	❑
	loss, destruction	_____ times in _____ years	❑	❑	❑
	interruption	_____ times in _____ years	❑	❑	❑
	disclosure	_____ times in _____ years	❑	❑	❑
	modification	_____ times in _____ years	❑	❑	❑
	loss, destruction	_____ times in _____ years	❑	❑	❑
	interruption	_____ times in _____ years	❑	❑	❑

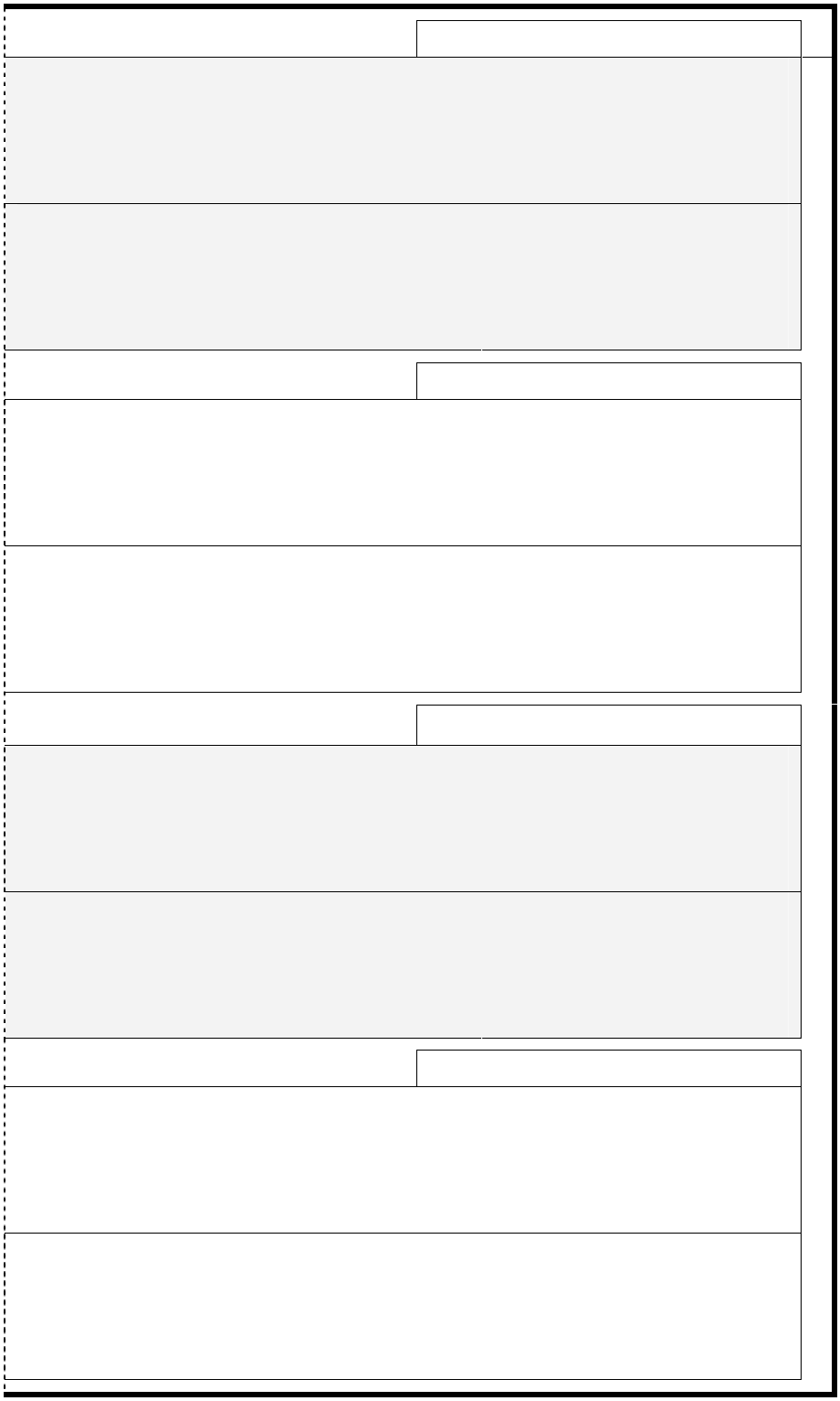
Threat Context | **Other Problems (cont.)**

Notes
What additional notes about each threat do you want to record?

Step 16

Other Problems (cont.)	**Areas of Concern**
Give examples of how _____ could affect the ability of this person or group of people to provide critical services, skills, and knowledge.	
Give examples of how _____ could affect the ability of this person or group of people to provide critical services, skills, and knowledge.	
Give examples of how _____ could affect the ability of this person or group of people to provide critical services, skills, and knowledge.	
Give examples of how _____ could affect the ability of this person or group of people to provide critical services, skills, and knowledge.	

Areas of Concern



4 Threat Translation Guide

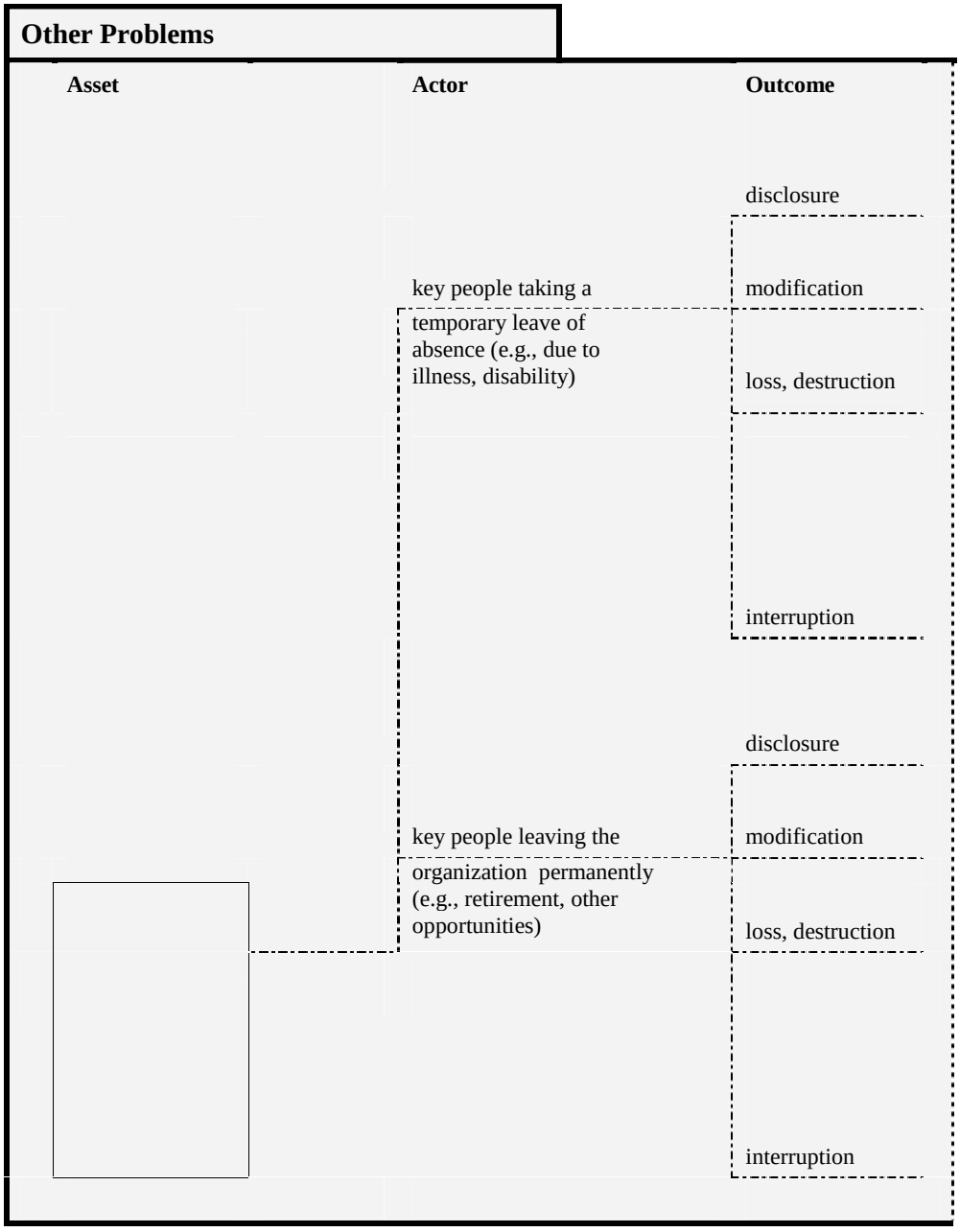
Phase 1
Process S2
Activity S2.3

Threat Translation Guide

The *Threat Translation Guide* describes each branch of an asset-based threat tree. If you have difficulty understanding the types of threats represented by a branch, you can use this guide to decipher the meaning of that branch.

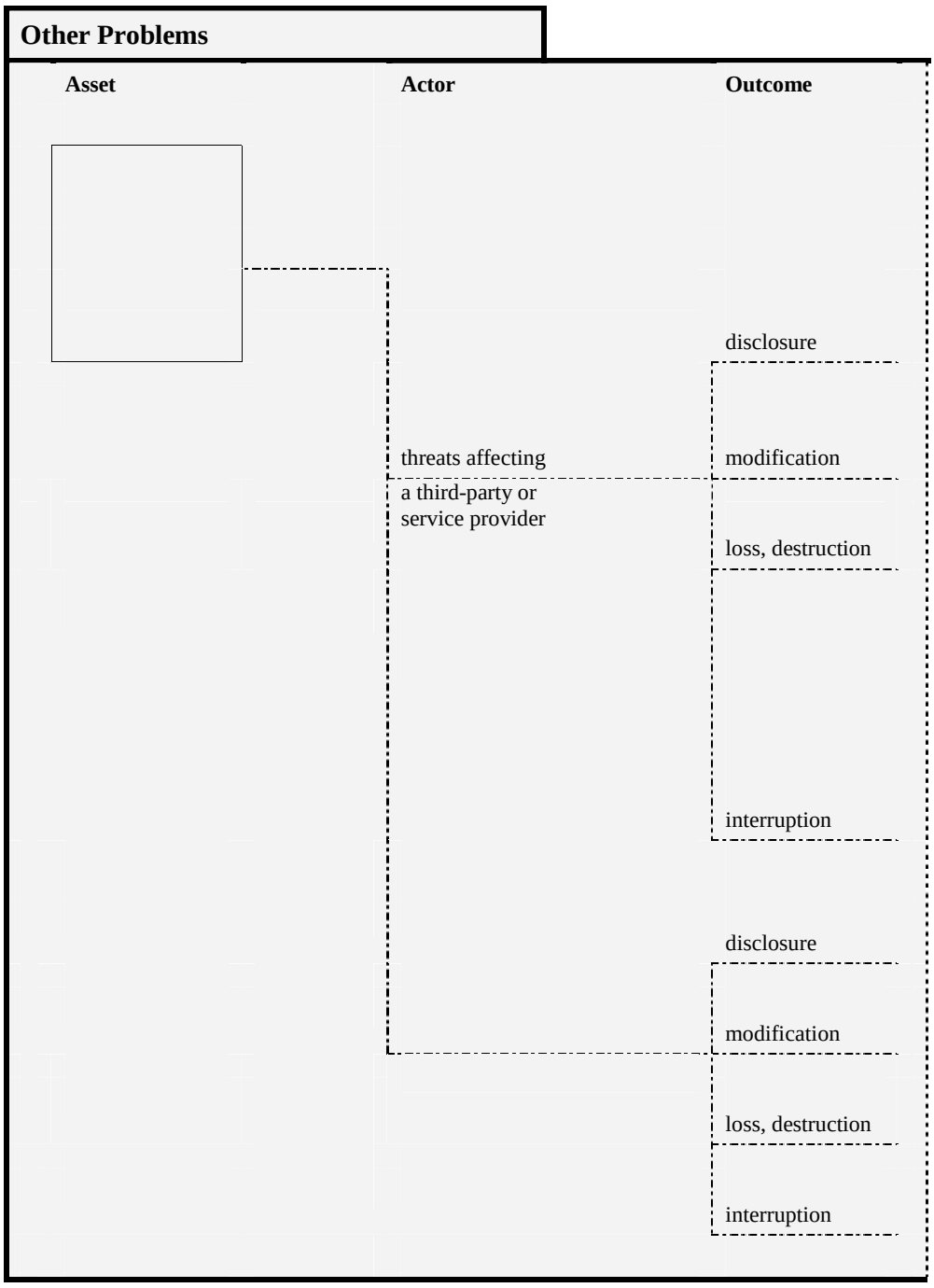
You will find asset-based threat trees for the following sources of threat:

Source of Threat	Page
Other problems	26-30



* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
---	---
---	---
---	---
A staff member(s) with unique knowledge or a unique skill takes a temporary leave of absence from an organization. The organization does not have any other staff members with comparable skills, resulting in an interruption of access to the unique knowledge or skill.	A key member of the IT group in a small organization takes a leave of absence to care for an ill family member. This member of the IT staff is responsible for maintaining a legacy order entry system. No other staff members know how to maintain the system. The organization has a temporary interruption of access to a vital skill that is important to its business operations.
---	---
---	---
---	---
A staff member(s) with unique knowledge or a unique skill leaves an organization permanently. The organization does not have any other staff members with comparable skills, resulting in an interruption of access to the unique knowledge or skill until a replacement if hired.	A clerk is responsible for entering data into a database system. The clerk, who is currently the only one at the company who understands how to use the system, unexpectedly leaves for a better position at another company. The organization no longer has access to a skill that is important to its business operations until a replacement is hired and trained.



* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
---	---
---	---
---	---
An organization depends on a third party for a particular service. Any threats to the third party that prevents them from fulfilling their obligations results in an interruption of service to the organization.	A service provider maintains the computing infrastructure for a manufacturing company. A shop floor scheduling system is physically located at the service provider's site. A disgruntled staff member employed by the service provider plants a software "time bomb" that takes down the service provider's networks for several days. The manufacturing site's access to the shop floor scheduling system is interrupted until the service provider can get its infrastructure running again.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
OCTAVE-S Implementation Guide, Version 1.0, Volume 8	F19628-00-C-0003

6. AUTHOR(S)

Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody

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

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

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

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

14. SUBJECT TERMS	15. NUMBER OF PAGES
information security, risk management, OCTAVE	30

16. PRICE CODE

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

OCTAVE®-S Implementation Guide, Version 1.0

Volume 9: Strategy and Plan Worksheets

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

HANDBOOK
CMU/SEI-2003-HB-003

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

OCTAVE®-S Implementation Guide, Version 1.0

Volume 9: Strategy and Plan Worksheets

CMU/SEI-2003-HB-003

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

Networked Systems Survivability Program

This report was prepared for the

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

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

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

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

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

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

Table of Contents

List of Tables

About This Document

This document is Volume 9 of the *OCTAVE-S Implementation Guide*, a 10-volume handbook supporting the OCTAVE-S methodology. This volume contains worksheets to record the organization's current and desired protection strategies and the risk mitigation plans.

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℠ (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 Introduction

This document contains the Operationally Critical Threat, Asset, and Vulnerability[SM] (OCTAVE[®])-S worksheets related to the organization's strategy development and planning activities.

Table 1 provides a brief introduction to the contents of this workbook, using activity step numbers as a key. For more details about how to complete each step, refer to the *OCTAVE[®]-S Method Guidelines*, which can be found in Volume 3 of the *OCTAVE[®]-S Implementation Guide*.

Table 1: Worksheets Provided in This Workbook

Step	Description	Worksheet	Activity	Pages
---	Document notes and recommendations identified during each step.	Notes and Recommendations	All Phases All Processes All Activities	3-12
---	Document action items identified during each step.	Action List	All Phases All Processes All Activities	13-22
Step 25	Transfer the stoplight status of each security practice area to the corresponding area of the *Protection Strategy worksheet*. For each security practice area, identify your organization's current approach for addressing that area.	Protection Strategy	Phase 3 Process S5 S5.1 Describe Current Protection Strategy	23-82

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

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

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 28	Develop mitigation plans for each security practice area selected during Step 27. As you complete this step, if you have difficulty coming up with potential mitigation activities for a security practice area, review examples of mitigation activities for that area in the *Mitigation Activities Guide*.	Mitigation Plan	Phase 3 Process S5 S5.3 Develop Risk Mitigation Plans	115-128
Step 29	Determine whether your mitigation plans affect your organization's protection strategy. Record any changes on the *Protection Strategy worksheet*. Next, review the protection strategy, including proposed changes. Determine whether you intend to make any additional changes to the protection strategy. Record any additional changes on the *Protection Strategy worksheet*.	Protection Strategy	Phase 3 Process S5 S5.4 Identify Changes to Protection Strategy	23-82
Step 30	Determine what your organization must do to implement the results of this evaluation and improve its security posture.	Next Steps	Phase 3 Process S5 S5.5 Identify Next Steps	129-132

2 Notes and Recommendations Worksheet

	All Phases All Processes All Activities
Throughout Evaluation	Document notes and recommendations identified during each step.

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Recommendation

What recommendations do you want to record?	*For which step is this recommendation relevant?*
	Step _____

Recommendation

What recommendations do you want to record?	*For which step is this recommendation relevant?*
	Step _____

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Recommendation	
What recommendations do you want to record?	*For which step is this recommendation relevant?*
	Step _____

Recommendation	
What recommendations do you want to record?	*For which step is this recommendation relevant?*
	Step _____

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Recommendation	
What recommendations do you want to record?	*For which step is this recommendation relevant?*
	Step _____

Recommendation	
What recommendations do you want to record?	*For which step is this recommendation relevant?*
	Step _____

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Recommendation	
What recommendations do you want to record?	*For which step is this recommendation relevant?*
	Step _____

Recommendation	
What recommendations do you want to record?	*For which step is this recommendation relevant?*
	Step _____

3 Action List Worksheet

	All Phases All Processes All Activities
Throughout Evaluation	Document action items identified during each step.

Action Item

	What actions do you intend to take? *Assign an identification number to each action item.*	*For which step is this action item relevant?*
ID # _____		Step _____

Action Item

	What actions do you intend to take? *Assign an identification number to each action item.*	*For which step is this action item relevant?*
ID # _____		Step _____

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?*
Completion Date:	*By when must the action item be completed?*
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?*
Completion Date:	*By when must the action item be completed?*
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

Action Item

ID #	*What actions do you intend to take?* *Assign an identification number to each action item.*	*For which step is this action item relevant?*
_____		Step _____

Action Item

ID #	*What actions do you intend to take?* *Assign an identification number to each action item.*	*For which step is this action item relevant?*
_____		Step _____

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?*
Completion Date:	*By when must the action item be completed?*
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?*
Completion Date:	*By when must the action item be completed?*
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

Action Item

ID #	*What actions do you intend to take?* *Assign an identification number to each action item.*	*For which step is this action item relevant?*
_____		Step _____

Action Item

ID #	*What actions do you intend to take?* *Assign an identification number to each action item.*	*For which step is this action item relevant?*
_____		Step _____

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?*
Completion Date:	*By when must the action item be completed?*
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?*
Completion Date:	*By when must the action item be completed?*
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

Action Item

ID #	*What actions do you intend to take?* *Assign an identification number to each action item.*	*For which step is this action item relevant?*
_____		Step _____

Action Item

ID #	*What actions do you intend to take?* *Assign an identification number to each action item.*	*For which step is this action item relevant?*
_____		Step _____

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?*
Completion Date:	*By when must the action item be completed?*
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?*
Completion Date:	*By when must the action item be completed?*
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

4 Protection Strategy Worksheet

	Phase 3 Process S5 Activity S5.1
Step 25	Transfer the stoplight status of each security practice area to the corresponding area of the *Protection Strategy worksheet*. For each security practice area, identify your organization's current approach for addressing that area.

	Phase 3 Process S5 Activity S5.4
Step 29	Determine whether your mitigation plans affect your organization's protection strategy. Record any changes on the *Protection Strategy worksheet*. Next, review the protection strategy, including proposed changes. Determine whether you intend to make any additional changes to the protection strategy. Record any additional changes on the *Protection Strategy worksheet*.

1. Security Awareness and Training

Stoplight Status ☐

Step 25: How formal is your organization's training strategy?

Step 29: Will any mitigation activities change your training strategy?
Do you want to make any additional changes to your training strategy?

Training Strategy	Step 25	Step 29
The organization has a documented training strategy that includes security awareness training and security-related training for supported technologies.	❑ Current	❑ Change
The organization has an informal and undocumented training strategy.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: How often is security awareness training provided?

Step 29: Will any mitigation activities change how often security awareness training is provided?
Do you want to make any additional changes to how often security awareness training is provided?

Security Awareness Training	Step 25	Step 29
Periodic security awareness training is provided for all employees _____time(s) every _____ years.	❑ Current	❑ Change
Security awareness training is provided for new staff members as part of their orientation activities.	❑ Current	❑ Change
The organization does not provide security awareness training. Staff members learn about security issues on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

1. Security Awareness and Training

Step 25: To what extent are IT staff members required to attend security-related training?

Step 29: Will any mitigation activities change the requirement for attending security-related training?
Do you want to make any additional changes to the requirement for attending security-related training?

Security-Related Training for Supported Technologies	Step 25	Step 29
Information technology staff members are required to attend security-related training for any technologies that they support.	❑ Current	❑ Change
Information technology staff members can attend security-related training for any technologies that they support if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for information technology staff members to attend security-related training for supported technologies. Information technology staff members learn about security-related issues on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: How formal is your organization's mechanism for providing periodic security updates?

Step 29: Will any mitigation activities change your mechanism for providing periodic security updates?
Do you want to make any additional changes to your mechanism for providing periodic security updates?

Periodic Security Updates	Step 25	Step 29
The organization has a formal mechanism for providing staff members with periodic updates/bulletins about important security issues.	❑ Current	❑ Change
The organization does not have a mechanism for providing staff members with periodic updates/bulletins about important security issues.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

1. Security Awareness and Training

Stoplight Status ☐

Step 25: How formal is your organization's mechanism for verifying that staff receives training?

Step 29: Will any mitigation activities change your mechanism for verifying that staff receives training?
Do you want to make any additional changes to your mechanism for verifying that staff receives training?

Training Verification	Step 25	Step 29
The organization has formal mechanisms for tracking and verifying that staff members receive appropriate security-related training.	❑ Current	❑ Change
The organization has informal mechanisms for tracking and verifying that staff members receive appropriate security-related training.	❑ Current	❑ Change
The organization has no mechanisms for tracking and verifying that staff members receive appropriate security-related training.	❑ Current	❑ Change
_____	❑ Current	❑ Change

Step 25: What additional characteristic of your current approach to security awareness and training do you want to record?

Step 29: Will any mitigation activities change this characteristic?
Do you want to make any additional changes to this characteristic?

Other:	Step 25	Step 29
_____	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____	❑ Current	❑ Change

2. Security Strategy

Stoplight Status ☐

Step 25: How formal is your organization's mechanism for integrating security and business strategies?

Step 29: Will any mitigation activities change your mechanism for integrating security and business strategies?
Do you want to make any additional changes to your mechanism for integrating security and business strategies?

Business and Security Strategy Integration	**Step 25**	**Step 29**
The organization has formal mechanisms for integrating • security considerations into business strategies • business strategies and goals into security strategies and policies	❑ Current	❑ Change
The organization has informal mechanisms for integrating • security considerations into business strategies • business strategies and goals into security strategies and policies	❑ Current	❑ Change
The organization has no mechanisms for integrating • security considerations into business strategies • business strategies and goals into security strategies and policies	❑ Current	❑ Change
_____ _____	❑ Current	❑ Change

Step 25: How formal are your organization's security strategies, goals, and objectives?

Step 29: Will any mitigation activities change your security strategies, goals, and objectives?
Do you want to make any additional changes to your security strategies, goals, and objectives?

Documented Strategies	**Step 25**	**Step 29**
The organization has documented security strategies, goals, and objectives.	❑ Current	❑ Change
The organization has a partial set of documented security strategies, goals, and objectives. Some aspects of security strategies, goals, and objectives are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented security strategies, goals, and objectives.	❑ Current	❑ Change
_____ _____	❑ Current	❑ Change

2. Security Strategy

Step 25: To what extent does your security awareness training program include information about the organization's security strategy?

Step 29: Will any mitigation activities change the content of your security awareness training to include strategy information?
Do you want to make any additional changes to the content of your security awareness training?

Staff Awareness	**Step 25**	**Step 29**
The organization's security awareness training program includes information about the organization's security strategy. This training is provided for all employees _____time(s) every _____ years.	❑ Current	❑ Change
The organization's security awareness training program includes information about the organization's security strategy. This training is provided for new staff members as part of their orientation activities.	❑ Current	❑ Change
The organization's security awareness training program does not include information about the organization's security strategy. Staff members learn about the organization's security strategy on their own.	❑ Current	❑ Change
_____ _____	❑ Current	❑ Change

Step 25: What additional characteristic of your current approach to security strategy do you want to record?

Step 29: Will any mitigation activities change this characteristic?
Do you want to make any additional changes to this characteristic?

Other:	**Step 25**	**Step 29**
_____ _____	❑ Current	❑ Change
_____ _____	❑ Current	❑ Change
_____ _____	❑ Current	❑ Change

3. Security Management

Stoplight Status ☐

Step 25: To what extent are security roles and responsibilities formally defined?

Step 29: Will any mitigation activities change the extent to which security roles and responsibilities are formally defined? Do you want to make any additional changes to how security roles and responsibilities are formally defined?

Roles and Responsibilities	Step 25	Step 29
The organization has formally documented information security roles and responsibilities for all staff in the organization.	❑ Current	❑ Change
The organization has formally documented information security roles and responsibilities for selected staff in the organization.	❑ Current	❑ Change
The organization has informal and undocumented information security roles and responsibilities.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent is security formally factored into your organization's budget?

Step 29: Will any mitigation activities change how security is formally factored into your organization's budget? Do you want to make any additional changes to how security is formally factored into your organization's budget?

Funding	Step 25	Step 29
The organization's budget has a distinct line item for information security activities. The funding level is determined based on a formal assessment of the organization's information security risks.	❑ Current	❑ Change
The organization's budget has a distinct line item for information security activities. The funding level is determined using informal processes.	❑ Current	❑ Change
The organization's budget explicitly includes information security activities under the line item for information technology (IT). The funding level is determined based on a formal assessment of the organization's information security risks.	❑ Current	❑ Change
The organization's budget explicitly includes information security activities under the line item for information technology. The funding level is determined using informal processes.	❑ Current	❑ Change
Neither the organization's budget nor the IT department's budget explicitly includes funding for information security activities.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

3. Security Management

Step 25: How formal are your organization's security-related human resource procedures?

Step 29: Will any mitigation activities change your security-related human resource procedures? Do you want to make any additional changes to your security-related human resource procedures?

Human Resource Procedures	Step 25	Step 29
The organization has formally defined procedures for including security considerations in the organization's hiring (e.g., background checks) and termination (e.g., removing access to all systems and information) processes.	❑ Current	❑ Change
The organization has some formally defined procedures for including security considerations in the organization's hiring (e.g., background checks) and termination (e.g., removing access to all systems and information) processes. Some procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented procedures for including security considerations in the organization's hiring (e.g., background checks) and termination (e.g., removing access to all systems and information) processes.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: How formal is your organization's process for managing information security risk?

Step 29: Will any mitigation activities change your process for managing information security risk? Do you want to make any additional changes to your process for managing information security risk?

Risk Management	Step 25	Step 29
The organization has a formally defined process for assessing and managing its information security risks.	❑ Current	❑ Change
The organization has a formally defined process for assessing its information security risks. The process for managing information security risks is informal and undocumented.	❑ Current	❑ Change
The organization has an informal and undocumented approach for assessing and managing its information security risks.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

3. Security Management

Stoplight Status ☐

Step 25: To what extent does your security-awareness training program include information about the organization's security management process?

Step 29: Will any mitigation activities change the content of your security awareness training to include security management information?
Do you want to make any additional changes to the content of your security awareness training?

Staff Awareness	Step 25	Step 29
The organization's security-awareness training program includes information about the organization's security management process. This training is provided for all employees _____time(s) every _____ years.	❑ Current	❑ Change
The organization's security-awareness training program includes information about the organization's security management process. This training is provided for new staff members as part of their orientation activities.	❑ Current	❑ Change
The organization's security-awareness training program does not include information about the organization's security management process. Staff members learn about security management on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: How formal is your organization's mechanism for providing managers with security-related information?

Step 29: Will any mitigation activities change how security-related information is provided to managers?
Do you want to make any additional changes to how security-related information is provided to managers?

Management Awareness	Step 25	Step 29
The organization has a formal mechanism for providing managers with summaries of important security-related information.	❑ Current	❑ Change
The organization has an informal and undocumented mechanism for providing managers with summaries of important security-related information.	❑ Current	❑ Change
The organization has no mechanism for providing managers with summaries of important security-related information.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

3. Security Management

Step 25: What additional characteristic of your current approach to security management do you want to record?

Step 29: Will any mitigation activities change this characteristic?
Do you want to make any additional changes to this characteristic?

Other:	**Step 25**	**Step 29**
_____ _____	❑ Current	❑ Change
_____ _____	❑ Current	❑ Change
_____ _____	❑ Current	❑ Change

4. Security Policies and Regulations

Stoplight Status

Step 25: To what extent are your organization's security-related policies formally documented?

Step 29: Will any mitigation activities change the extent to which your security-related policies are formally documented? Do you want to make any additional changes to the formality and documentation of your security-related policies?

Documented Policies	Step 25	Step 29
The organization has a comprehensive set of formally documented security-related policies.	❑ Current	❑ Change
The organization has a partial set of formally documented security-related policies. Some security-related policies are informal and undocumented.	❑ Current	❑ Change
The organization's security-related policies are informal and undocumented.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: How formal is your organization's mechanism for creating and updating its security-related policies?

Step 29: Will any mitigation activities change how security-related policies are created and updated? Do you want to make any additional changes to how security-related policies are created and updated?

Policy Management	Step 25	Step 29
The organization has a formal mechanism for creating and updating its security-related policies.	❑ Current	❑ Change
The organization has a formal mechanism for creating its security-related policies. The organization has an informal and undocumented mechanism for updating its security-related policies.	❑ Current	❑ Change
The organization has an informal and undocumented mechanism for creating and updating its security-related policies.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

4. Security Policies and Regulations

Step 25: How formal are your organization's procedures for enforcing its security-related policies?

Step 29: Will any mitigation activities change how security-related policies are enforced?
Do you want to make any additional changes to how security-related policies are enforced?

Policy Enforcement	Step 25	Step 29
The organization has formal procedures for enforcing its security-related policies. Enforcement procedures are consistently followed.	❑ Current	❑ Change
The organization has formal procedures for enforcing its security-related policies. Enforcement procedures are inconsistently followed.	❑ Current	❑ Change
The organization has informal and undocumented procedures for enforcing its security-related policies.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your security-awareness training program include information about the organization's security policies and regulations?

Step 29: Will any mitigation activities change the content of your security awareness training to include security policy and regulation information?
Do you want to make any additional changes to the content of your security awareness training?

Staff Awareness	Step 25	Step 29
The organization's security-awareness training program includes information about the organization's security policies and regulations. This training is provided for all employees _____time(s) every _____ years.	❑ Current	❑ Change
The organization's security-awareness training program includes information about the organization's security policies and regulations. This training is provided for new staff members as part of their orientation activities.	❑ Current	❑ Change
The organization's security-awareness training program does not include information about the organization's security policies and regulations. Staff members learn about security policies and regulations on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

4. Security Policies and Regulations

Stoplight Status ☐

Step 25: How formal are your organization's procedures for complying with security-related policies and regulations?

Step 29: Will any mitigation activities change how your organization complies with security-related policies and regulations?
Do you want to make any additional changes to how your organization complies with security-related policies and regulations?

Policy and Regulation Compliance	Step 25	Step 29
The organization has formal procedures for complying with information security policies, applicable laws and regulations, and insurance requirements.	❑ Current	❑ Change
The organization has formal procedures for complying with certain information security policies, applicable laws and regulations, and insurance requirements. Some procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented procedures for complying with information security policies, applicable laws and regulations, and insurance requirements.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: What additional characteristic of your current approach to security policies and regulations do you want to record?

Step 29: Will any mitigation activities change this characteristic?
Do you want to make any additional changes to this characteristic?

Other:	Step 25	Step 29
_____	❑ Current	❑ Change
_____		
_____	❑ Current	❑ Change
_____		
_____	❑ Current	❑ Change
_____		

5. Collaborative Security Management

Stoplight Status ☐

*Step 25: How formal are your organization's policies and procedures for protecting information when working with **collaborators and partners**?*

Step 29: Will any mitigation activities change the policies and procedures for protecting information when working with collaborators and partners?
Do you want to make any additional changes to the policies and procedures for protecting information when working with collaborators and partners?

Collaborators and Partners	Step 25	Step 29
The organization has documented policies and procedures for protecting information when working with collaborators and partners.	❑ Current	❑ Change
The organization has documented policies and procedures for protecting certain information when working with collaborators and partners. The organization has informal and undocumented policies and procedures for protecting other types of information when working with collaborators and partners.	❑ Current	❑ Change
The organization has informal and undocumented policies and procedures for protecting information when working with collaborators and partners.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

*Step 25: How formal are your organization's policies and procedures for protecting information when working with **contractors and subcontractors**?*

Step 29: Will any mitigation activities change the policies and procedures for protecting information when working with contractors and subcontractors?
Do you want to make any additional changes to the policies and procedures for protecting information when working with contractors and subcontractors?

Contractors and Subcontractors	Step 25	Step 29
The organization has documented policies and procedures for protecting information when working with contractors and subcontractors.	❑ Current	❑ Change
The organization has documented policies and procedures for protecting certain information when working with contractors and subcontractors. The organization has informal and undocumented policies and procedures for protecting other types of information when working with contractors and subcontractors.	❑ Current	❑ Change
The organization has informal and undocumented policies and procedures for protecting information when working with contractors and subcontractors.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

5. Collaborative Security Management

*Step 25: How formal are your organization's policies and procedures for protecting information when working with **service providers**?*

Step 29: Will any mitigation activities change the policies and procedures for protecting information when working with service providers?
Do you want to make any additional changes to the policies and procedures for protecting information when working with service providers?

Service Providers	Step 25	Step 29
The organization has documented policies and procedures for protecting information when working with service providers.	❑ Current	❑ Change
The organization has documented policies and procedures for protecting certain information when working with service providers. The organization has informal and undocumented policies and procedures for protecting other types of information when working with service providers.	❑ Current	❑ Change
The organization has informal and undocumented policies and procedures for protecting information when working with service providers.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization formally communicate its information protection requirements to third parties?

Step 29: Will any mitigation activities change how your organization communicates its information protection requirements to third parties?
Do you want to make any additional changes to how your organization communicates its information protection requirements to third parties?

Requirements	Step 25	Step 29
The organization documents information protection requirements and explicitly communicates them to all appropriate third parties.	❑ Current	❑ Change
The organization informally communicates information protection requirements to all appropriate third parties.	❑ Current	❑ Change
The organization does not communicate information protection requirements to third parties.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

5. Collaborative Security Management

Stoplight Status ☐

Step 25: To what extent does your organization verify that third parties are addressing information protection requirements?

Step 29: Will any mitigation activities change verification mechanisms?
Do you want to make any additional changes to verification mechanisms?

Verification	Step 25	Step 29
The organization has formal mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.	❑ Current	❑ Change
The organization has informal mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.	❑ Current	❑ Change
The organization has no mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your security-awareness training program include information about collaborative security management?

Step 29: Will any mitigation activities change the content of your security awareness training to include information about collaborative security management?
Do you want to make any additional changes to the content of your security awareness training?

Staff Awareness	Step 25	Step 29
The organization's security-awareness training program includes information about the organization's collaborative security management policies and procedures. This training is provided for all employees _____time(s) every _____ years.	❑ Current	❑ Change
The organization's security-awareness training program includes information about the organization's collaborative security management policies and procedures. This training is provided for new staff members as part of their orientation activities.	❑ Current	❑ Change
The organization's security-awareness training program does not include information about the organization's collaborative security management policies and procedures. Staff members learn about collaborative security management policies and procedures on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

5. Collaborative Security Management

Step 25: What additional characteristic of your current approach to collaborative security management do you want to record?

Step 29: Will any mitigation activities change this characteristic?
Do you want to make any additional changes to this characteristic?

Other:	**Step 25**	**Step 29**
_____ _____	❑ Current	❑ Change
_____ _____	❑ Current	❑ Change
_____ _____	❑ Current	❑ Change

6. Contingency Planning/Disaster Recovery

Stoplight Status ☐

Step 25: To what extent has an analysis of operations, applications, and data criticality been performed?

Step 29: Will any mitigation activities change the extent to which business operations are analyzed? Do you want to make any additional changes to business operations analysis?

Business Operations Analysis	Step 25	Step 29
An analysis of operations, applications, and data criticality has been performed.	❑ Current	❑ Change
A partial analysis of operations, applications, and data criticality has been performed.	❑ Current	❑ Change
An analysis of operations, applications, and data criticality has not been performed.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent has your organization documented its contingency plans?

Step 29: Will any mitigation activities change how contingency plans are documented? Do you want to make any additional changes to contingency plan documentation?

Documented Plans	Step 25	Step 29
The organization has documented business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	❑ Current	❑ Change
The organization has partially documented business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies. Some aspects of the plans are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

6. Contingency Planning/Disaster Recovery

Step 25: To what extent has your organization tested its contingency plans?

Step 29: Will any mitigation activities change how contingency plans are tested?
Do you want to make any additional changes to contingency plan testing?

Tested Plans	Step 25	Step 29
The organization has formally tested its business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	❑ Current	❑ Change
The organization has informally tested its business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	❑ Current	❑ Change
The organization has not tested its business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent is physical and electronic access to critical information formally factored into contingency plans?

Step 29: Will any mitigation activities change the extent to which information access is formally factored into contingency plans?
Do you want to make any additional changes to how information access is formally factored into contingency plans?

Information Access	Step 25	Step 29
Physical and electronic access to critical information is formally factored into the organization's contingency, disaster recovery, and business continuity plans.	❑ Current	❑ Change
Physical and electronic access to some critical information is formally factored into the organization's contingency, disaster recovery, and business continuity plans. Other types of critical information are not formally factored into the plans.	❑ Current	❑ Change
Physical and electronic access to critical information is not formally factored into the organization's contingency, disaster recovery, and business continuity plans.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

6. Contingency Planning/Disaster Recovery

Stoplight Status ☐

Step 25: To what extent does your security-awareness training program include information about contingency planning and disaster recovery?

Step 29: Will any mitigation activities change the content of your security awareness training to include information about contingency planning and disaster recovery?
Do you want to make any additional changes to the content of your security awareness training?

Staff Awareness	**Step 25**	**Step 29**
The organization's security-awareness training program includes information about the organization's contingency, disaster recovery, and business continuity plans. This training is provided for all employees _____time(s) every _____ years.	❑ Current	❑ Change
The organization's security-awareness training program includes information about the organization's contingency, disaster recovery, and business continuity plans. This training is provided for new staff members as part of their orientation activities.	❑ Current	❑ Change
The organization's security-awareness training program does not include information about the organization's contingency, disaster recovery, and business continuity plans. Staff members learn about contingency, disaster recovery, and business continuity plans on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change

Step 25: What additional characteristic of your current approach to contingency planning and disaster recovery do you want to record?

Step 29: Will any mitigation activities change this characteristic?
Do you want to make any additional changes to this characteristic?

Other:	**Step 25**	**Step 29**
_____	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____	❑ Current	❑ Change

7. Physical Access Control

Stoplight Status ☐

Step 25: Who is currently responsible for physical access control?

Step 29: Will any mitigation activities change responsibility for physical access control?
Do you want to make any additional changes affecting responsibility for physical access control?

Responsibility	**Step 25**			**Step 29**		
	❑ Current			❑ Change		
Task	Internal	External	Combined	Internal	External	Combined
Controlling physical access to the building and premises (e.g., controlling visitor access)	❑	❑	❑	❑	❑	❑
Controlling physical access to work areas (e.g., controlling staff and visitor access)	❑	❑	❑	❑	❑	❑
Controlling physical access to IT hardware	❑	❑	❑	❑	❑	❑
Controlling physical access to software media	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑

7. Physical Access Control

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area? Do you want to make any additional changes to how procedures are documented for this area?

Procedures	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented plans and procedures for controlling physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization has some formally documented policies and procedures for controlling physical access to the building and premises, work areas, IT hardware, and software media. Some policies and procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented plans and procedures for controlling physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area? Do you want to make any additional changes to the requirement for attending training in this area?

Training	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
Designated staff members are required to attend training that includes a review of the organization's plans and procedures for physical access control.	❑ Current	❑ Change
Designated staff members can attend training that includes a review of the organization's plans and procedures for physical access control if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for designated staff members to attend training that includes a review of the organization's plans and procedures for physical access control. Designated staff members learn about physical access control on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

7. Physical Access Control

Stoplight Status ☐

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for physical access control are formally communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization's requirements for physical access control are informally communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization's requirements for physical access control are not communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for physical access control.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for physical access control.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for physical access control.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

7. Physical Access Control

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for physical access control are formally communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization's requirements for physical access control are informally communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization's requirements for physical access control are not communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for physical access control.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for physical access control.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for physical access control.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

8. Monitoring and Auditing Physical Security

Stoplight Status ☐

Step 25: Who is currently responsible for monitoring and auditing physical security?

Step 29: Will any mitigation activities change responsibility for monitoring and auditing physical security? Do you want to make any additional changes affecting responsibility for monitoring and auditing physical security?

Responsibility	**Step 25**			**Step 29**		
	❑ Current			❑ Change		
Task	Internal	External	Combined	Internal	External	Combined
Keeping maintenance records to document repairs and modifications to IT hardware	❑	❑	❑	❑	❑	❑
Monitoring physical access to controlled IT hardware	❑	❑	❑	❑	❑	❑
Monitoring physical access to controlled IT software media	❑	❑	❑	❑	❑	❑
Monitoring physical access to restricted work areas	❑	❑	❑	❑	❑	❑
Reviewing monitoring records on a periodic basis	❑	❑	❑	❑	❑	❑
Investigating and addressing any unusual activity that is identified	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑

8. Monitoring and Auditing Physical Security

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area? Do you want to make any additional changes to how procedures are documented for this area?

Procedures	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented plans and procedures for monitoring physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization has some formally documented policies and procedures for monitoring physical access to the building and premises, work areas, IT hardware, and software media. Some policies and procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented plans and procedures for monitoring physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area? Do you want to make any additional changes to the requirement for attending training in this area?

Training	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
Designated staff members are required to attend training for monitoring physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
Designated staff members can attend training for monitoring physical access to the building and premises, work areas, IT hardware, and software media if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for designated staff members to attend training for monitoring physical access to the building and premises, work areas, IT hardware, and software media. Designated staff members learn about monitoring physical access on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

8. Monitoring and Auditing Physical Security

Stoplight Status ☐

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for monitoring physical security are formally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization's requirements for monitoring physical security are informally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization's requirements for monitoring physical security are not communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for monitoring physical security.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for monitoring physical security.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for monitoring physical security.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

8. Monitoring and Auditing Physical Security

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for monitoring physical security are formally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization's requirements for monitoring physical security are informally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization's requirements for monitoring physical security are not communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for monitoring physical security.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for monitoring physical security.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for monitoring physical security.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

9. System and Network Management

Stoplight Status

Step 25: Who is currently responsible for system and network management?

Step 29: Will any mitigation activities change responsibility for system and network management?
Do you want to make any additional changes affecting responsibility for system and network management?

Responsibility	**Step 25**			**Step 29**		
	❑ Current			❑ Change		
Task	Internal	External	Combined	Internal	External	Combined
Configuring IT hardware and software	❑	❑	❑	❑	❑	❑
Securely storing sensitive information (e.g., backups stored off site, process for discarding sensitive information)	❑	❑	❑	❑	❑	❑
Checking the integrity of installed software	❑	❑	❑	❑	❑	❑
Keeping systems up to date with respect to revisions, patches, and recommendations in security advisories	❑	❑	❑	❑	❑	❑
Making and tracking changes to IT hardware and software	❑	❑	❑	❑	❑	❑
Managing passwords, accounts, and privileges	❑	❑	❑	❑	❑	❑
Selecting system and network management tools	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑

9. System and Network Management

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area? Do you want to make any additional changes to how procedures are documented for this area?

Procedures	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented system and network management procedures.	❑ Current	❑ Change
The organization has some formally documented system and network management procedures. Some procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented system and network management procedures.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area? Do you want to make any additional changes to the requirement for attending training in this area?

Training	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
Information technology staff members are required to attend training for managing systems and networks and using system and network management tools.	❑ Current	❑ Change
Information technology staff members can attend training for managing systems and networks and using system and network management tools if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for information technology staff members to attend training for managing systems and networks and using system and network management tools. Information technology staff members learn about system and network management on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

9. System and Network Management

Stoplight Status ☐

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's security-related system and network management requirements are formally communicated to all contractors and service providers that maintain systems and networks.	❑ Current	❑ Change
The organization's security-related system and network management requirements are informally communicated to all contractors and service providers that maintain systems and networks.	❑ Current	❑ Change
The organization's security-related system and network management requirements are not communicated to all contractors and service providers that maintain systems and networks.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for security-related system and network management.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for security-related system and network management.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for security-related system and network management.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

9. System and Network Management

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's security-related system and network management requirements are formally communicated to all contractors and service providers that maintain systems and networks.	❑ Current	❑ Change
The organization's security-related system and network management requirements are informally communicated to all contractors and service providers that maintain systems and networks.	❑ Current	❑ Change
The organization's security-related system and network management requirements are not communicated to all contractors and service providers that maintain systems and networks.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for security-related system and network management.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for security-related system and network management.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for security-related system and network management.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

10. Monitoring and Auditing IT Security

Stoplight Status ☐

Step 25: Who is currently responsible for monitoring and auditing IT security?

Step 29: Will any mitigation activities change responsibility for monitoring and auditing IT security?
Do you want to make any additional changes affecting responsibility for monitoring and auditing IT security?

Responsibility	**Step 25**			**Step 29**		
	❑ Current			❑ Change		
Task	Internal	External	Combined	Internal	External	Combined
Using system and network monitoring tools to track system and network activity	❑	❑	❑	❑	❑	❑
Auditing the firewall and other security components periodically for compliance with policy	❑	❑	❑	❑	❑	❑
Investigating and addressing any unusual activity that is identified	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑

10. Monitoring and Auditing IT Security

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area? Do you want to make any additional changes to how procedures are documented for this area?

Procedures	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented procedures for monitoring network-based access to systems and networks.	❑ Current	❑ Change
The organization has some formally documented procedures for monitoring network-based access to systems and networks. Some procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented procedures for monitoring network-based access to systems and networks.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area? Do you want to make any additional changes to the requirement for attending training in this area?

Training	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
Information technology staff members are required to attend training for monitoring network-based access to systems and networks and using monitoring and auditing tools.	❑ Current	❑ Change
Information technology staff members can attend training for monitoring network-based access to systems and networks and using monitoring and auditing tools if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for information technology staff members to attend training for monitoring network-based access to systems and networks and using monitoring and auditing tools. Information technology staff members learn about monitoring systems and networks on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

10. Monitoring and Auditing IT Security

Stoplight Status ☐

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	**Step 25**	**Step 29**
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for monitoring information technology security are formally communicated to all contractors and service providers that monitor systems and networks.	❑ Current	❑ Change
The organization's requirements for monitoring information technology security are informally communicated to all contractors and service providers that monitor systems and networks.	❑ Current	❑ Change
The organization's requirements for monitoring information technology security are not communicated to all contractors and service providers that monitor systems and networks.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	**Step 25**	**Step 29**
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for monitoring information technology security.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for monitoring information technology security.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for monitoring information technology security.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

10. Monitoring and Auditing IT Security

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for monitoring information technology security are formally communicated to all contractors and service providers that monitor systems and networks.	❑ Current	❑ Change
The organization's requirements for monitoring information technology security are informally communicated to all contractors and service providers that monitor systems and networks.	❑ Current	❑ Change
The organization's requirements for monitoring information technology security are not communicated to all contractors and service providers that monitor systems and networks.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for monitoring information technology security.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for monitoring information technology security.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for monitoring information technology security.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

11. Authentication and Authorization

Stoplight Status

Step 25: Who is currently responsible for authentication and authorization?

Step 29: Will any mitigation activities change responsibility for authentication and authorization? Do you want to make any additional changes affecting responsibility for authentication and authorization?

Responsibility	**Step 25**			**Step 29**		
	❑ Current			❑ Change		
Task	Internal	External	Combined	Internal	External	Combined
Implementing access controls (e.g., file permissions, network configuration) to restrict user access to information, sensitive systems, specific applications and services, and network connections	❑	❑	❑	❑	❑	❑
Implementing user authentication (e.g., passwords, biometrics) to restrict user access to information, sensitive systems, specific applications and services, and network connections	❑	❑	❑	❑	❑	❑
Establishing and terminating access to systems and information for both individuals and groups	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑

11. Authentication and Authorization

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area? Do you want to make any additional changes to how procedures are documented for this area?

Procedures	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented authorization and authentication procedures for restricting user access to information, sensitive systems, specific applications and services, and network connections.	❑ Current	❑ Change
The organization has some formally documented authorization and authentication procedures for restricting user access to information, sensitive systems, specific applications and services, and network connections. Some procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented authorization and authentication procedures for restricting user access to information, sensitive systems, specific applications and services, and network connections.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area? Do you want to make any additional changes to the requirement for attending training in this area?

Training	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
Information technology staff members are required to attend training for implementing technological measures to restrict user access to information, sensitive systems, specific applications and services, and network connections.	❑ Current	❑ Change
Information technology staff members can attend training for implementing technological measures to restrict user access to information, sensitive systems, specific applications and services, and network connections if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for information technology staff members to attend training for implementing technological measures to restrict user access to information, sensitive systems, specific applications and services, and network connections. Information technology staff members learn about authentication and authorization on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

11. Authentication and Authorization

Stoplight Status ☐

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for controlling access to systems and information are formally communicated to all contractors and service providers that provide authentication and authorization services.	❑ Current	❑ Change
The organization's requirements for controlling access to systems and information are informally communicated to all contractors and service providers that monitor systems and networks.	❑ Current	❑ Change
The organization's requirements for controlling access to systems and information are not communicated to all contractors and service providers that monitor systems and networks.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for authentication and authorization.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for authentication and authorization.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for authentication and authorization.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

11. Authentication and Authorization

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for controlling access to systems and information are formally communicated to all contractors and service providers that provide authentication and authorization services.	❑ Current	❑ Change
The organization's requirements for controlling access to systems and information are informally communicated to all contractors and service providers that monitor systems and networks.	❑ Current	❑ Change
The organization's requirements for controlling access to systems and information are not communicated to all contractors and service providers that monitor systems and networks.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for authentication and authorization.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for authentication and authorization.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for authentication and authorization.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

12. Vulnerability Management

Stoplight Status ☐

Step 25: Who is currently responsible for vulnerability management?

Step 29: Will any mitigation activities change responsibility for vulnerability management?
Do you want to make any additional changes affecting responsibility for vulnerability management?

Responsibility	**Step 25**			**Step 29**		
	❑ Current			❑ Change		
Task	Internal	External	Combined	Internal	External	Combined
Selecting vulnerability evaluation tools, checklists, and scripts	❑	❑	❑	❑	❑	❑
Scheduling and performing technology vulnerability evaluations on a periodic basis	❑	❑	❑	❑	❑	❑
Keeping up to date with known vulnerability types and attack methods	❑	❑	❑	❑	❑	❑
Reviewing sources of information on vulnerability announcements, security alerts, and notices	❑	❑	❑	❑	❑	❑
Interpreting the results of technology vulnerability evaluations	❑	❑	❑	❑	❑	❑
Addressing technology vulnerabilities that are identified	❑	❑	❑	❑	❑	❑
Maintaining secure storage and disposition of technology vulnerability data	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑

12. Vulnerability Management

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area? Do you want to make any additional changes to how procedures are documented for this area?

Procedures	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented vulnerability management procedures.	❑ Current	❑ Change
The organization has some formally documented vulnerability management procedures. Some procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented vulnerability management procedures.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area? Do you want to make any additional changes to the requirement for attending training in this area?

Training	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
Information technology staff members are required to attend training for managing technology vulnerabilities and using vulnerability evaluation tools.	❑ Current	❑ Change
Information technology staff members can attend training for managing technology vulnerabilities and using vulnerability evaluation tools if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for information technology staff members to attend training for managing technology vulnerabilities and using vulnerability evaluation tools. Information technology staff members learn about vulnerability management on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

12. Vulnerability Management

Stoplight Status ☐

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's vulnerability management requirements are formally communicated to all contractors and service providers that manage technology vulnerabilities.	❑ Current	❑ Change
The organization's vulnerability management requirements are informally communicated to all contractors and service providers that manage technology vulnerabilities.	❑ Current	❑ Change
The organization's vulnerability management requirements are not communicated to all contractors and service providers that manage technology vulnerabilities.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for vulnerability management.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for vulnerability management.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for vulnerability management.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

12. Vulnerability Management

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's vulnerability management requirements are formally communicated to all contractors and service providers that manage technology vulnerabilities.	❑ Current	❑ Change
The organization's vulnerability management requirements are informally communicated to all contractors and service providers that manage technology vulnerabilities.	❑ Current	❑ Change
The organization's vulnerability management requirements are not communicated to all contractors and service providers that manage technology vulnerabilities.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for vulnerability management.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for vulnerability management.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for vulnerability management.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

13. Encryption

Stoplight Status ☐

Step 25: Who is currently responsible for encryption?

Step 29: Will any mitigation activities change responsibility for encryption?
Do you want to make any additional changes affecting responsibility for encryption?

Responsibility	**Step 25**			**Step 29**		
	❑ Current			❑ Change		
Task	Internal	External	Combined	Internal	External	Combined
Implementing encryption technologies to protect sensitive information that is electronically stored and transmitted (e.g., data encryption, public key infrastructure, virtual private network technology)	❑	❑	❑	❑	❑	❑
Implementing encrypted protocols for remotely managing systems, routers, and firewalls	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area?
Do you want to make any additional changes to how procedures are documented for this area?

Procedures	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented procedures for implementing and using encryption technologies.	❑ Current	❑ Change
The organization has some formally documented procedures for implementing and using encryption technologies. Some procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented procedures for implementing and using encryption technologies.	❑ Current	❑ Change
_____ _____	❑ Current	❑ Change

13. Encryption

Step 25: To what extent are IT staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area?
Do you want to make any additional changes to the requirement for attending training in this area?

Information Technology Staff Training	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
Information technology staff members are required to attend training for implementing encryption technologies.	❑ Current	❑ Change
Information technology staff members can attend training for implementing encryption technologies if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for information technology staff members to attend training for implementing encryption technologies. Information technology staff members learn about implementing encryption technologies on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area?
Do you want to make any additional changes to the requirement for attending training in this area?

Staff Training	**Step 25**	**Step 29**
All staff members are required to attend training for using encryption technologies.	❑ Current	❑ Current
All staff members can attend training for using encryption technologies if they request it.	❑ Current	❑ Current
The organization generally does not provide opportunities for staff members to attend training for using encryption technologies. Staff members learn about using encryption technologies on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

13. Encryption

Stoplight Status ☐

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for protecting sensitive information are formally communicated to all contractors and service providers that provide encryption technologies.	❑ Current	❑ Change
The organization's requirements for protecting sensitive information are informally communicated to all contractors and service providers that provide encryption technologies.	❑ Current	❑ Change
The organization's requirements for protecting sensitive information are not communicated to all contractors and service providers that provide encryption technologies.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for implementing encryption technologies.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for implementing encryption technologies.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for implementing encryption technologies.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

13. Encryption

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for protecting sensitive information are formally communicated to all contractors and service providers that provide encryption technologies.	❑ Current	❑ Change
The organization's requirements for protecting sensitive information are informally communicated to all contractors and service providers that provide encryption technologies.	❑ Current	❑ Change
The organization's requirements for protecting sensitive information are not communicated to all contractors and service providers that provide encryption technologies.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for implementing encryption technologies.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for implementing encryption technologies.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for implementing encryption technologies.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

14. Security Architecture and Design

Stoplight Status ☐

Step 25: Who is currently responsible for security architecture and design?

Step 29: Will any mitigation activities change responsibility for security architecture and design?
Do you want to make any additional changes affecting responsibility for security architecture and design?

Responsibility	**Step 25**			**Step 29**		
	❑ Current			❑ Change		
Task	Internal	External	Combined	Internal	External	Combined
Designing security controls in new and revised systems and networks	❑	❑	❑	❑	❑	❑
Documenting and revising diagrams that show the enterprise-wide security architecture and network topology	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑

14. Security Architecture and Design

Step 25: To what extent are practices for this area formally documented?

Step 29: Will any mitigation activities change the extent to which practices are formally documented for this area? Do you want to make any additional changes to how practices are documented for this area?

Procedures	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented security architecture and design practices.	❑ Current	❑ Change
The organization has some formally documented security architecture and design practices. Some practices in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented security architecture and design practices.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area? Do you want to make any additional changes to the requirement for attending training in this area?

Training	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
Staff members are required to attend training for designing secure systems and networks.	❑ Current	❑ Change
Staff members can attend training for designing secure systems and networks if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for staff members to attend training for designing secure systems and networks. Staff members learn about security architecture and design on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

14. Security Architecture and Design

Stoplight Status ☐

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's security-related requirements are formally communicated to all contractors and service providers that design systems and networks.	❑ Current	❑ Change
The organization's security-related requirements are informally communicated to all contractors and service providers that design systems and networks.	❑ Current	❑ Change
The organization's security-related requirements are not communicated to all contractors and service providers that design systems and networks.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for security architecture and design.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for security architecture and design.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for security architecture and design.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

14. Security Architecture and Design

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's security-related requirements are formally communicated to all contractors and service providers that design systems and networks.	❑ Current	❑ Change
The organization's security-related requirements are informally communicated to all contractors and service providers that design systems and networks.	❑ Current	❑ Change
The organization's security-related requirements are not communicated to all contractors and service providers that design systems and networks.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for security architecture and design.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for security architecture and design.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for security architecture and design.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

15. Incident Management

Stoplight Status ☐

Step 25: Who is currently responsible for incident management?

Step 29: Will any mitigation activities change responsibility for incident management?
Do you want to make any additional changes affecting responsibility for incident management?

Responsibility	**Step 25**			**Step 29**		
	❑ Current			❑ Change		
Task	Internal	External	Combined	Internal	External	Combined
Documenting and revising procedures for identifying, reporting, and responding to suspected security incidents and violations	❑	❑	❑	❑	❑	❑
Documenting and revising policies and procedures for working with law enforcement agencies	❑	❑	❑	❑	❑	❑
Testing incident management procedures on a periodic basis	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑

15. Incident Management

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area? Do you want to make any additional changes to how procedures are documented for this area?

Procedures	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented incident management procedures.	❑ Current	❑ Change
The organization has some formally documented incident management procedures. Some procedures in this area are informal and undocumented.	❑ Current	❑ Change
The organization has informal and undocumented incident management procedures.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area? Do you want to make any additional changes to the requirement for attending training in this area?

Training	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
Designated staff members are required to attend training for incident management.	❑ Current	❑ Change
Designated staff members can attend training for incident management if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for designated staff members to attend training for incident management. Designated staff members learn about incident management on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

15. Incident Management

Stoplight Status ☐

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for managing incidents are formally communicated to all contractors and service providers that provide incident management services.	❑ Current	❑ Change
The organization's requirements for managing incidents are informally communicated to all contractors and service providers that provide incident management services.	❑ Current	❑ Change
The organization's requirements for managing incidents are not communicated to all contractors and service providers that provide incident management services.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for managing incidents.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for managing incidents.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for managing incidents.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

15. Incident Management

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for managing incidents are formally communicated to all contractors and service providers that provide incident management services.	❑ Current	❑ Change
The organization's requirements for managing incidents are informally communicated to all contractors and service providers that provide incident management services.	❑ Current	❑ Change
The organization's requirements for managing incidents are not communicated to all contractors and service providers that provide incident management services.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for managing incidents.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for managing incidents.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for managing incidents.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

5 Mitigation Activities Guide

Phase 3
Process S5
Activity S5.3

Mitigation Activities Guide	The *Mitigation Activities Guide* describes potential mitigation activities for each security practice area. You will find examples of mitigation activities related to each security practice area in this guide.

1. Security Awareness and Training	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Develop and document a training strategy that includes security awareness training and security-related training for supported technologies.	Training Strategy
Provide periodic security awareness training for *all* employees on a periodic basis (e.g., _____time(s) every _____ years).	Security Awareness Training
Provide security awareness training for *new* staff members as part of their orientation activities.	Security Awareness Training
Require IT staff members to attend security-related training for any technologies that they support.	Security-Related Training for Supported Technologies
Enable IT staff members to attend security-related training for any technologies that they support.	Security-Related Training for Supported Technologies
Implement a *formal* mechanism for providing staff members with periodic updates/bulletins about important security issues.	Periodic Security Updates
Implement an *informal* mechanism for providing staff members with periodic updates/bulletins about important security issues.	Periodic Security Updates
Implement a *formal* mechanism for tracking and verifying that staff members receive appropriate security-related training.	Training Verification
Implement an *informal* mechanism for tracking and verifying that staff members receive appropriate security-related training.	Training Verification
Schedule a one-time offering of security awareness training.	---
Send selected staff members to training for a specific technology (i.e., a limited or one-time offering in a specific technology).	---
Cross train selected staff members to use specific information systems and/or applications. Cross-trained staff members will back up the primary users of those systems and/or applications.	---
Cross train selected staff members to provide specific skills or services. Cross-trained staff members will back up the staff members who normally provide those skills or services.	---
Cross train selected IT staff members to configure and maintain specific information systems, networks, and/or applications. Cross-trained IT staff members will back up the primary administrators who normally maintain those systems, networks, and/or applications.	---
Ensure that selected staff members understand how to notify and work with third parties that own or operate key systems. These people will be able to work with third parties when there are problems with systems owned and/or operated by those third parties.	---

2. Security Strategy	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Implement a *formal* mechanism for integrating • security considerations into business strategies • business strategies and goals into security strategies and policies	Business and Security Strategy Integration
Implement an *informal* mechanism for integrating • security considerations into business strategies • business strategies and goals into security strategies and policies	Business and Security Strategy Integration
Document security strategies, goals, and objectives for *all* aspects of information security.	Documented Strategies
Document the security strategies, goals, and objectives for *selected* security-related areas.	Documented Strategies
Incorporate information about the organization's security strategy into the organization's security-awareness training program.	Staff Awareness

3. Security Management	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Document information security roles and responsibilities for *all* staff in the organization.	Roles and Responsibilities
Document information security roles and responsibilities for *selected* staff members.	Roles and Responsibilities
Include a separate line item for information security activities in the *organization's budget*.	Funding
Include a separate line item for information security activities in organization's *information technology budget*.	Funding
Use the results of an information security risk evaluation to determine the level of funding for information security activities.	Funding
Document procedures for including security considerations in the organization's hiring and termination processes.	Human Resource Procedures
Document a process for *assessing and managing* the organization's information security risks.	Risk Management
Document a process for *assessing* the organization's information security risks.	Risk Management
Incorporate information about the organization's security management process into the organization's security-awareness training program.	Staff Awareness
Implement a *formal* mechanism for providing managers with summaries of important security-related information.	Management Awareness
Implement an *informal* mechanism for providing managers with summaries of important security-related information.	Management Awareness

4. Security Policies and Regulations **Candidate Mitigation Activities**

Mitigation Activity	Protection Strategy Link
Document a *comprehensive* set of security-related policies.	Documented Policies
Document security-related policies for *selected areas.*	Documented Policies
Implement a formal mechanism for *creating and updating* security-related policies.	Policy Management
Implement a formal mechanism for *creating* security-related policies.	Policy Management
Implement formal procedures for enforcing security-related policies.	Policy Enforcement
Incorporate information about the organization's security policies and regulations into the organization's security-awareness training program.	Staff Awareness
Document procedures for complying with *all* information security policies, applicable laws and regulations, and insurance requirements.	Policy and Regulation Compliance
Document procedures for complying with *selected* security policies, applicable laws and regulations, and insurance requirements.	Policy and Regulation Compliance

5. Collaborative Security Management **Candidate Mitigation Activities**

Mitigation Activity	Protection Strategy Link
Document policies and procedures for protecting information when working with collaborators and partners.	Collaborators and Partners
Document policies and procedures for protecting information when working with contractors and subcontractors.	Contractors and Subcontractors
Document policies and procedures for protecting information when working with service providers.	Service Providers
Implement a *formal* mechanism (e.g., contract mechanism) for communicating information protection requirements to all appropriate third parties.	Requirements
Implement an *informal* mechanism (e.g., assign responsibility) for communicating information protection requirements to all appropriate third parties.	Requirements
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet the organization's information protection requirements.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet the organization's information protection requirements.	Verification
Incorporate information about the organization's policies and procedures for collaborative security management into the organization's security-awareness training program.	Staff Awareness

6. Contingency Planning/Disaster Recovery	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Perform an analysis defining the criticality of *all* operations, applications, and data.	Business Operations Analysis
Perform an analysis defining the criticality of *selected* operations, applications, and/or data.	Business Operations Analysis
Document business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	Documented Plans
Document *a subset of the following plans* for responding to emergencies: business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s).	Documented Plans
Formally test the organization's business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	Tested Plans
Formally test a *subset of the following plans* for responding to emergencies: business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s).	Tested Plans
Incorporate contingency plans into the organization's disaster recovery and business continuity plans for accessing critical information.	Information Access
Incorporate information about the organization's contingency, disaster recovery, and business continuity plans into the organization's security-awareness training program.	Staff Awareness
Document a disaster recovery plan for a specific system maintained by the information technology staff.	---
Develop a disaster recovery plan for a specific system maintained by a third party.	---
Document a business continuity plan for specific business processes.	---
Purchase insurance for any security problems related to a specific system.	---
Configure and maintain a hot backup for a system.	---
Configure and maintain a cold backup for a specific system.	---

7. Physical Access Control	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Change responsibility for controlling physical access to the building and premises (e.g., controlling visitor access).	Responsibility
Change responsibility for controlling physical access to work areas (e.g., controlling staff and visitor access).	Responsibility
Change responsibility for controlling physical access to IT hardware.	Responsibility
Change responsibility for controlling physical access to software media.	Responsibility
Document formal procedures for controlling physical access to the building and premises, work areas, IT hardware, and software media.	Procedures
Send selected staff members to training for controlling physical access to the building and premises, work areas, IT hardware, and software media.	Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for physical access control to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for physical access control to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for physical access control have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for physical access control have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities	7. Physical Access Control
Mitigation Activity	**Protection Strategy Link**
Develop procedures for controlling physical access to • the building and premises • selected work areas • IT hardware • software media • other	---
Rearrange office/work spaces to restrict physical access to systems, computers, or other devices by unauthorized personnel.	---
Implement sign-in sheets to manage visitors' access to the building and/or designated work areas.	---
Implement card access to restrict physical access to the building.	---
Implement card access to restrict physical access to specific work areas.	---
Replace door locks in specific work areas.	---
Retain the services of security guards to protect the premises.	---
Rearrange the physical setup of computing equipment in specific areas to counteract environmental threats.	---
Perform an audit of physical security to identify security weaknesses in the physical infrastructure.	---
Develop procedures for specific systems defining the designated time that a device can remain logged on before that device is automatically locked or logged off.	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for controlling physical access in the organization and to verify that those requirements have been met.	---

8. Monitoring and Auditing Physical Security — **Candidate Mitigation Activities**

Mitigation Activity	Protection Strategy Link
Change responsibility for keeping maintenance records that document repairs and modifications to IT hardware.	Responsibility
Change responsibility for monitoring physical access to controlled IT hardware	Responsibility
Change responsibility for monitoring physical access to controlled IT software media.	Responsibility
Change responsibility for monitoring physical access to restricted work areas.	Responsibility
Change responsibility for reviewing monitoring records on a periodic basis.	Responsibility
Change responsibility for investigating and addressing any unusual activity that is identified.	Responsibility
Document formal procedures for monitoring physical access to the building and premises, work areas, IT hardware, and software media.	Procedures
Send selected staff members to training for monitoring physical access to the building and premises, work areas, IT hardware, and software media.	Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for monitoring physical security to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for monitoring physical security to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for monitoring physical security have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for monitoring physical security have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities | **8. Monitoring and Auditing Physical Security**

Mitigation Activity	Protection Strategy Link
Install video cameras in designated areas of the premises.	---
Retain the services of security guards to monitor activity on the premises.	---
Implement sign-in sheets to log visitors' access to the building and/or designated work areas.	---
Implement card access to log physical access to the building and/or designated work areas.	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for monitoring physical security in the organization and to verify that those requirements have been met.	---

9. System and Network Management	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Change responsibility for configuring IT hardware and software.	Responsibility
Change responsibility for securely storing sensitive information (e.g., backups stored off site, process for discarding sensitive information).	Responsibility
Change responsibility for checking the integrity of installed software.	Responsibility
Change responsibility for keeping systems up to date with respect to revisions, patches, and recommendations in security advisories.	Responsibility
Change responsibility for making and tracking changes to IT hardware and software.	Responsibility
Change responsibility for managing passwords, accounts, and privileges.	Responsibility
Change responsibility for selecting system and network management tools.	Responsibility
Document formal procedures for managing systems and networks.	Procedures
Send selected staff members to training for managing systems and networks.	Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for secure system and network management to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for secure system and network management to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for secure system and network management have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for secure system and network management have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities	9. System and Network Management
Mitigation Activity	**Protection Strategy Link**
Check the configuration of IT hardware and software on specific systems.	---
Check the integrity of installed software on specific systems.	---
Check specific systems to ensure that they are up to date with respect to revisions, patches, and recommendations in security advisories.	---
Check specific systems for default accounts and accounts that are no longer used.	---
Check specific systems for easy-to-crack passwords.	---
Check specific systems to see if they are running unnecessary services.	---
Check specific systems for the presence of viruses or other malicious code.	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for securely managing systems and networks in the organization and to verify that those requirements have been met.	---

10. Monitoring and Auditing IT Security **Candidate Mitigation Activities**

Mitigation Activity	Protection Strategy Link
Change responsibility for using system and network monitoring tools to track system and network activity.	Responsibility
Change responsibility for periodically auditing the firewall and other security components for compliance with policy.	Responsibility
Change responsibility for investigating and addressing any unusual activity that is identified.	Responsibility
Document formal procedures for monitoring network access to systems and networks.	Procedures
Send selected staff members to training for monitoring network access to systems and networks.	Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for monitoring IT security to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for monitoring IT security to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for monitoring IT security have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for monitoring IT security have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities	10. Monitoring and Auditing IT Security
Mitigation Activity	**Protection Strategy Link**
Develop procedures for • reviewing system logs • using system and network monitoring tools to track system activity • auditing the firewall and other security components periodically for compliance with policy • investigating and addressing any unusual activity that is identified	---
Implement an intrusion detection system and assign an IT staff member the responsibility of tracking network activity.	---
Perform an audit of the firewall and other security components to ensure that they are compliant with the organization's security policies.	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for monitoring IT security in the organization and to verify that those requirements have been met.	---

11. Authentication and Authorization — **Candidate Mitigation Activities**

Mitigation Activity	Protection Strategy Link
Change responsibility for implementing access controls (e.g., file permissions, network configuration) to restrict user access to information, sensitive systems, specific applications and services, and network connections.	Responsibility
Change responsibility for implementing user authentication (e.g., passwords, biometrics) to restrict user access to information, sensitive systems, specific applications and services, and network connections.	Responsibility
Change responsibility for establishing and terminating access to systems and information for both individuals and groups.	Responsibility
Document formal procedures for restricting user access to information, sensitive systems, specific applications and services, and network connections.	Procedures
Send selected staff members to training for implementing technological measures to restrict user access to information, sensitive systems, specific applications and services, and network connections.	Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for controlling access to systems and information to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for controlling access to systems and information to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for controlling access to systems and information have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for controlling access to systems and information have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities | **11. Authentication and Authorization**

Mitigation Activity	Protection Strategy Link
Check access controls (e.g., file permissions, network configuration) on specific systems.	---
Check that appropriate authentication mechanisms (e.g., passwords, biometrics) are used to restrict user access to specific systems.	---
Check specific systems for easy-to-crack passwords.	---
Check specific systems to ensure that all devices that access those systems automatically timeout after a designated period of time.	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for controlling access to systems and information in the organization and to verify that those requirements have been met.	---

12. Vulnerability Management	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Change responsibility for selecting vulnerability evaluation tools, checklists, and scripts.	Responsibility
Change responsibility for scheduling and performing technology vulnerability evaluations on a periodic basis.	Responsibility
Change responsibility for keeping up to date with known vulnerability types and attack methods.	Responsibility
Change responsibility for reviewing sources of information on vulnerability announcements, security alerts, and notices.	Responsibility
Change responsibility for interpreting the results of technology vulnerability evaluations.	Responsibility
Change responsibility for addressing technology vulnerabilities that are identified.	Responsibility
Change responsibility for maintaining secure storage and disposition of technology vulnerability data.	Responsibility
Document formal procedures for managing technology vulnerabilities.	Procedures
Send selected staff members to training for managing technology vulnerabilities.	Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for managing technology vulnerabilities to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for managing technology vulnerabilities to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for managing technology vulnerabilities have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for managing technology vulnerabilities have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities	12. Vulnerability Management
Mitigation Activity	**Protection Strategy Link**
Check specific systems for technology vulnerabilities.	---
Perform an audit of information technology security to identify security weaknesses in the computing infrastructure.	---
Contract with an outside organization to attack your organization's systems and network via the Internet (i.e., penetration testing, red team).	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for managing technology vulnerabilities in the organization and to verify that those requirements have been met.	---

13. Encryption	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Change responsibility for implementing encryption technologies to protect sensitive information that is electronically stored and transmitted (e.g., data encryption, public key infrastructure, virtual private network technology).	Responsibility
Change responsibility for implementing encrypted protocols for remotely managing systems, routers, and firewalls.	Responsibility
Change responsibility for implementing encrypted protocols for remotely managing systems, routers, and firewalls.	Responsibility
Document formal procedures for implementing and using encryption technologies.	Procedures
Send selected IT staff members to training for implementing encryption technologies.	Information Technology Staff Training
Send selected staff members to training for using encryption technologies.	Staff Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for protecting sensitive information to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for protecting sensitive information to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for protecting sensitive information have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for protecting sensitive information have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities	13. Encryption
Mitigation Activity	**Protection Strategy Link**
Implement encryption technologies to protect specific types of information and/or systems.	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for protecting sensitive information in the organization and to verify that those requirements have been met.	---

14. Security Architecture and Design — **Candidate Mitigation Activities**

Mitigation Activity	Protection Strategy Link
Change responsibility for designing security controls in new and revised systems and networks.	Responsibility
Change responsibility for documenting and revising diagrams that show the enterprise-wide security architecture and network topology.	Responsibility
Document formal security architecture and design practices.	Procedures
Send selected staff members to training for designing secure systems and networks.	Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for incorporating appropriate security features into systems and networks to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for incorporating appropriate security features into systems and networks to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for incorporating appropriate security features into systems and networks have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for incorporating appropriate security features into systems and networks have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities	14. Security Architecture and Design
Mitigation Activity	**Protection Strategy Link**
Update the design of specific systems to include appropriate security controls.	---
Investigate periodic crashes of specific systems and correct any design problems that lead to those crashes.	---
Document or update diagrams that show the enterprise-wide security architecture and network topology.	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for incorporating appropriate security features into systems and networks and to verify that those requirements have been met.	---

15. Incident Management	Candidate Mitigation Activities
Mitigation Activity	**Protection Strategy Link**
Change responsibility for documenting and revising procedures for identifying, reporting, and responding to suspected security incidents and violations.	Responsibility
Change responsibility for documenting and revising policies and procedures for working with law enforcement agencies.	Responsibility
Change responsibility for testing incident management procedures on a periodic basis.	Responsibility
Document formal procedures for managing incidents.	Procedures
Send selected staff members to training for managing incidents.	Training
Implement a *formal* mechanism (e.g., contract mechanism) for communicating the organization's requirements for managing incidents to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement an *informal* mechanism (e.g., assign responsibility) for communicating the organization's requirements for managing incidents to all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Collaborative Issues
Implement a *formal* mechanism (e.g., contract mechanism) for verifying that the organization's requirements for managing incidents have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification
Implement an *informal* mechanism (e.g., assign responsibility) for verifying that the organization's requirements for managing incidents have been met by all appropriate contractors, service providers, and third parties. Assign responsibility for working directly with those contractors, service providers, and third parties to selected staff members.	Verification

Candidate Mitigation Activities	15. Incident Management
Mitigation Activity	**Protection Strategy Link**
Test current incident management procedures.	---
Arrange a meeting with all appropriate contractors, service providers, and third parties to communicate requirements for managing incidents in the organization and to verify that those requirements have been met.	---

6 Mitigation Plan Worksheet

	Phase 3 Process S5 Activity S5.3
Step 28	Develop mitigation plans for each security practice area selected during Step 27. As you complete this step, if you have difficulty coming up with potential mitigation activities for a security practice area, review examples of mitigation activities for that area in the *Mitigation Activities Guide*.

Mitigation Area: _____

Step 28

Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*

Mitigation Area: _____

Step 28

Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*

Mitigation Area: _____

Step 28

Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*

Mitigation Area: _____

Step 28

Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*

Mitigation Area: _____

Step 28

Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*

Mitigation Area: _____

Step 28

Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*

7 Next Steps Worksheet

	Phase 3 Process S5 Activity S5.5
Step 30	Determine what your organization must do to implement the results of this evaluation and improve its security posture.

Step 30

Management Sponsorship for Security Improvement

What must management do to support the implementation of OCTAVE-S results?

Consider the following:

- Contribute funds to information security activities.
- Assign staff to information security activities.
- Ensure that staff members have sufficient time allocated to information security activities.
- Enable staff to receive training about information security.
- Make information security a strategic priority.

Monitoring Implementation
What will the organization do to track progress and ensure that the results of this evaluation are implemented?

Expanding the Current Information Security Risk Evaluation
Will you expand the current OCTAVE-S evaluation to include additional critical assets? Which ones?

Next Information Security Risk Evaluation
When will the organization conduct its next OCTAVE-S evaluation?

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
OCTAVE-S Implementation Guide, Version 1.0, Volume 9	F19628-00-C-0003

6. AUTHOR(S)

Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody

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

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

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

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

14. SUBJECT TERMS	15. NUMBER OF PAGES
information security, risk management, OCTAVE	132

16. PRICE CODE

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

OCTAVE®-S Implementation Guide, Version 1.0

Volume 10: Example Scenario

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

HANDBOOK
CMU/SEI-2003-HB-003

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

OCTAVE®-S Implementation Guide, Version 1.0

Volume 10: Example Scenario

CMU/SEI-2003-HB-003

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

Networked Systems Survivability Program

This report was prepared for the

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

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

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

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

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

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

Table of Contents

List of Figures

About This Document

This document is Volume 10 of the *OCTAVE-S Implementation Guide*, a 10-volume handbook supporting the OCTAVE-S methodology. This volume provides complete example scenario of a fictitious medical facility, MedSite, and the results of its OCTAVE-S evaluation. Most of the worksheets showing the example results are provided. However, the complete worksheets for only one asset (rather than five) are included.

The other 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 MedSite Background

To help you understand how to complete the individual steps in this evaluation, we provide an example that illustrates how each step was conducted by personnel in a fictitious small medical facility called MedSite. The first two sections, including this one, provide background on MedSite and a commentary about how the evaluation proceeded at MedSite. The rest of this document consists of OCTAVE-S worksheets showing the results achieved by the MedSite analysis team. The background provides the necessary context to understand the contents of the worksheets and should be read in conjunction with the worksheets.

1.1 MedSite Description

MedSite is a hospital with several clinics and labs, some of which are at remote locations. The hospital includes the following functional areas:

- a permanent administrative organization
- permanent and temporary medical personnel, including physicians, surgeons, and medical staff
- permanent and temporary maintenance personnel, including facility and maintenance staff
- a small information technology department (three people) that is responsible for on-site computer and network maintenance and upgrades and for help desk activities (e.g., handling simple user requests)

1.2 MedSite's Organizational Structure

The MedSite Administrator is the chief administrator for the hospital. The chief administrator has a small staff that is responsible for overseeing operations at MedSite. Each major functional area of the organization (administrative, medical, and lab) reports directly to the chief administrator. MedSite's senior management team includes the MedSite Administrator and the individuals who lead the functional areas of the organization. Each functional area of MedSite contains one or more operational areas. The head of each operational area is considered to be a middle manager in the organization. Figure 1 shows the organizational chart for MedSite.

1.3 MedSite's System

MedSite's main information system is the Patient Information Data System (PIDS). PIDS is a distributed database application and system software with a dedicated PIDS server on a shared network accessed by both dedicated and shared desktop personal computers (PCs). The shared components support a variety of medical applications and databases. The system also links and integrates a set of smaller, older databases related to patient care, lab results, and billing.

Patient data can be entered into PIDS or one of the other databases at any time from any workstation. Physicians, administrative clerks, lab technicians, and nurses have authorization to enter data into PIDS as well as the other systems. Personal computers, or workstations, are located in all offices, treatment rooms (including emergency rooms), nursing stations, and labs. In addition, physicians can also remotely access PIDS using their home personal computers. In fact, there is talk around the hospital that medical personnel will soon be able to access PIDS using personal digital assistants (PDAs).

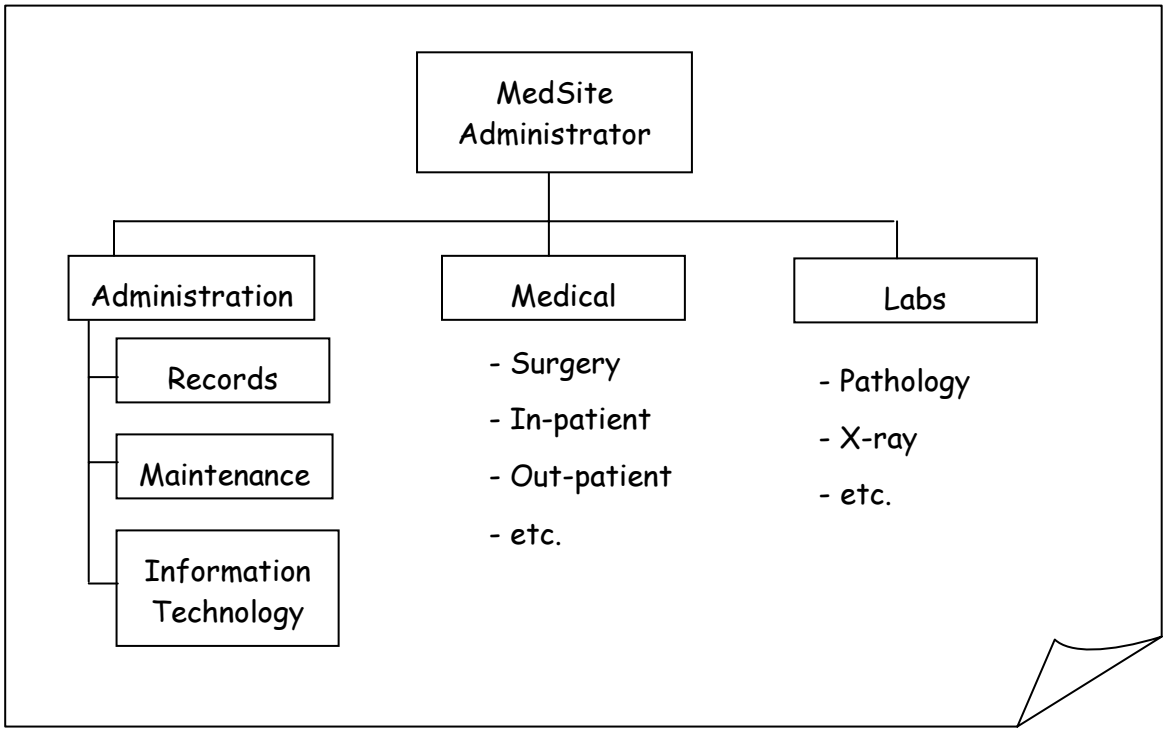


Figure 1: High-Level MedSite Organizational Chart

An independent contractor, ABC Systems, provides support for most of the systems at MedSite as well as for the network. MedSite's information technology (IT) personnel provide day-to-day maintenance under the training and direction of ABC Systems personnel. MedSite's IT staff also support the help desk by taking calls and responding to immediate needs. The IT staff members from MedSite provide on-site help desk support and basic system maintenance. ABC Systems provided MedSite's IT personnel with limited systems and network training about a year ago.

MedSite's senior managers decided they wanted a comprehensive review of information security within their facility. Several new regulations are now in effect (e.g., the Health Insurance Portability and Accountability Act [HIPAA]), requiring MedSite to document the results of an information security risk evaluation. The regulations also require MedSite to implement a practice-based standard of due care. After some discussion and consultation with other medical facility managers, they decided to use OCTAVE-S.

The analysis team has been selected and trained. The core analysis team members are

- Alvarez – a physician, at MedSite for five years
- Green – assistant manager of Administration, at MedSite for eight years. Green will lead the analysis team.
- Smith – senior IT staff member, at MedSite for three years
- Haley – lab technician, at MedSite for four years

The team met to prepare for the evaluation. They decided to scope the evaluation to include the entire organization as there are only three real operational areas – Administration, Medical, and the Lab. They also checked with colleagues in other medical facilities to locate any historical data on any type of threats that they might be willing to share later on or to discuss when the analysis team needed to define probability evaluation criteria. Probability is required by some regulations, and the team felt that they needed to try to use some form of qualitative probability during risk analysis.

As this was their first use of OCTAVE-S, they decided not to tailor the catalog of practices or the surveys to align them with current regulations, such as HIPAA. Instead, after the evaluation, they will use a gap analysis to determine what additional actions are required to ensure compliance and to protect their information-related assets. The budget for security improvements over the next six months is limited, and senior managers prefer to ensure their critical assets are protected now and deal with any additional regulation compliance during the next budget cycle.

1.4 MedSite Team's Experience

MedSite's analysis team completed the evaluation in four weeks working part time. This section summarizes the team's activities, its decisions, and other contextual information related to the evaluation. As you review the results, you will notice that we provide complete results for only one of the critical assets.

1.4.1 Phase 1: Build Asset-Based Threat Profiles

The analysis team met daily over the course of one week to finish Phase 1. At the end of the week, the team met with MedSite's senior managers to review the impact evaluation criteria and get them approved. MedSite's senior managers decided to use the criteria developed by the team and subsequently review the results. If the criteria turned out to be too vague or if they seemed to skew the results, senior managers reserved the right to revise the criteria and ask the team to re-evaluate the risks.

1.4.1.1 Process S1: Identify Organizational Information

S1.1: Establish impact evaluation criteria (Step 1)

Using the *Impact Evaluation Criteria Worksheet* [p. 33], the analysis team defined the ranges of possible impacts on the organization. The team had sufficient information on the nature of impacts caused by common problems and emergencies, and it used this information as the basis for setting impact measures (high, medium, low) across multiple impact areas. For example, MedSite is a very successful company, with more than 75% of the region's people coming to MedSite for medical care. MedSite normally sees a 5-15% fluctuation in patient numbers from month to month. The team uses this information to determine that the company could recover from a 10% drop in customers, but a 30% drop would mean a serious problem that could be irreversible. MedSite's budget includes a 2% margin for unexpected changes in operating costs and a 5% margin for unexpected changes in overall revenue. Insurance covers nearly all types of losses of up to $250,000 and many items up to $1 million without any increase in premiums. Any coverable loss of more than $1 million means an immediate increase in premiums. In terms of production, minor increases (10% for a few days) in personnel hours happen all the time because of accidents and unexpected fluctuations in patient needs. A high increase occurred during the previous year when a snowstorm nearly paralyzed the community. Nearly everyone at MedSite worked an additional 30% for a 3-day period to make up for lost time. The team also determined that any loss of life or permanent damage to patients was considered unacceptable. These items were incorporated into the evaluation criteria.

S1.2: Identify organizational assets (Step 2)

The analysis team used its knowledge of MedSite's systems as a starting point for identifying assets, because staff members' daily tasks were tightly integrated with the systems they used. When using the *Asset Identification Worksheet* [p. 45] to identify assets, team members could see how much information actually resided on MedSite's information systems. Patient information, which was regulated in terms of privacy and security, could be found in several forms including both electronic and paper files. The team also noticed that personal computers were common to all systems and provided a conduit to all important electronic information. It was more difficult for the team to identify people-related assets, because everyone had important roles at MedSite.

Eventually, the team decided that only people with unique skills or knowledge that could not easily be replaced would be documented as assets during the evaluation. They were essentially interested in identifying single points of failure related to people. For example, Smith was the only IT staff member with networking skills and was thus critical to day-to-day operations. Likewise the people at ABC Systems were also identified as important people-related assets. The staff at ABC Systems maintained PIDS for MedSite, and it would be difficult to find any other contracting organization that could easily assume this responsibility without disrupting MedSite's operations. In addition, ABC Systems was also in the midst of developing the replacement for PIDS (PIDS II), making ABC Systems integral to the future operations of MedSite as well.

S1.3: Evaluate organizational security practices (Steps 3-4)

The team used the *Security Practices Worksheet* [p. 51] to document the current state and effectiveness of their security practices. Team members discussed each survey question until they arrived at a consensus (Step 3a) about the extent to which each practice was present at MedSite. As they discussed a practice, team members often recorded notes about particular strengths and weaknesses (Step 3b) related to that practice. Finally, for each security practice area, the team assigned it a stoplight status based on the information it recorded (Step 4). The team was surprised at how many areas were assigned red and yellow statuses. Team members did not assign a green status to any of the security practice areas.

The team noted that some security practices were performed well at MedSite, but the vast majority were not executed properly. One of the few practices performed consistently well was documenting and revising policies. Because MedSite's policies were audited periodically, management paid particular attention to this practice area. Unfortunately, medical regulations had not specified the need for security in the past, and MedSite's security-related policies were incomplete. The team believed that physical security practices were adequate and assigned MedSite a yellow status for physical access control. However, monitoring and auditing physical security was assigned a red status. Team members were also concerned that the Facilities Management Group was so independent that it functioned like a separate entity, providing little communication and insight into its actions. After discussing the Facilities Management Group's physical security practices, the analysis team decided to add an additional concern to the collaborative security management security practice area.

Because ABC Systems maintained and controlled PIDS and other systems, the team had a difficult time answering some of the technology-based survey questions. In fact, no one at MedSite really understood what ABC Systems was doing, driving home how dependent MedSite had become on that contracting organization. Team members were also becoming increasingly concerned over the in-progress development of PIDS II.

Even though the majority of answers for the incident management area were negative, this was one area in which MedSite had a good set of documented procedures. The procedures were a standard, tested, and verified set provided by a medical society to which MedSite belonged. As a result, the team gave the company a yellow status for that area.

No other notes or action items resulted from Process S1.

1.4.1.2 Process S2: Create Threat Profiles

S2.1: Select Critical Assets (Steps 5 – 9)

Selecting critical assets proved to be less difficult that the analysis team expected. The team selected the following critical assets:

- PIDS (Patient Information Data System) – This was an obvious choice for the team. PIDS is central to MedSite's medical operations, because it is the central repository for patient-identifiable information. In addition, MedSite must comply with regulations for protecting the privacy of and securing electronic patient information.
- Paper medical records – These records are somewhat less important than PIDS, because MedSite is trying to move away from its reliance on paper medical records. However, the migration will take several years. In the meantime, the team decided that paper records also constituted a critical asset, because those records contain patient-identifiable information and are subject to privacy regulations.
- ABC Systems – MedSite has become reliant upon the information technology (IT) services provided by ABC Systems, MedSite's main IT contractor. ABC Systems maintains PIDS and other systems for MedSite and is also developing PIDS II, the replacement for PIDS. ABC Systems was an obvious choice as a critical asset given the importance of PIDS, PIDS II, and MedSite's ongoing efforts to become a paperless environment. ABC Systems is also typical of other types of contracting done by MedSite.
- Personal computers (PCs) – The analysis team noted that personal computers were common to all systems, providing a conduit to all important electronic information.
- ECDS (Emergency Care Data System) – This system was selected because it is representative of many smaller systems used at MedSite.

The analysis team recorded its choices for critical assets on the *Critical Asset Selection Worksheet* [p. 83].The team then started a *Critical Asset Workbook* for each critical asset (Step 6). It also recorded its rationale for selecting each asset (Step 7) as well as who uses and is responsible for each critical asset (Step 8) on each asset's *Critical Asset Information Worksheet* [p. 87]. Information about asset relationships had already been recorded on the *Asset Identification Worksheet* and was transcribed to the *Critical Asset Information Worksheet* (Step 9).

S2.2: Identify security requirements for critical assets (Steps 10 – 11)

Team members discussed which qualities of each asset were important to protect. This discussion resulted in the identification of security requirements for each critical asset, which were recorded on the appropriate *Critical Asset Information Worksheets* (Step 10) [p. 87]. Selecting the most important security requirement was frequently difficult, requiring significant discussion. For example, team members spent a lot of time discussing which security requirement for PIDS was most important (Step 11). After a healthy debate, the team selected availability of patient information as the most important security requirement for PIDS because the health and safety of patients require immediate and continuous access to patient information on PIDS. Confidentiality was also considered to be important, but it lacked the life and health implications of availability. Most of the issues surrounding confidentiality were actually related to regulations. The team decided that when making tradeoffs, the availability of medical information ultimately trumped violations of privacy laws.

S2.3: Identify threats to critical assets (Steps 12 – 16)

The analysis team then began constructing a threat profile for each critical asset, recording the profile on the appropriate *Risk Profile Worksheets* [pp. 91 and 131]. Team members consulted the appropriate *Threat Translation Guide* (Volumes 5-8) to ensure they actually understood the implied threats. For PIDS (using Volume 6 for systems assets), the team believed that all of the branches for the *human actors using network* and *physical access* trees were active, non-negligible threats (Step 12). Team members came to this conclusion based on their experiences and known issues related to network and physical security. The team believed that most threats from the *system problems* category would typically affect only the availability of information on PIDS. The exception to this was malicious code, which could result in any outcome. Threats from the *other problems* category were also believed to affect only the availability of PIDS.

For ABC Systems, the nature of the threats was quite different, because it is a different type of asset (people) than PIDS (system). The team was really concerned about only one type of threat – not having qualified, timely support from ABC Systems personnel. This was the only threat that the team recorded for ABC Systems.

For PIDS, the team identified the types of people who might be considered threat actors (Step 13). The team documented a broad range of potential actors, including hackers, disgruntled employees, and ABC Systems' personnel. With no insight into how ABC Systems handled access to confidential information or violations of security, the team was concerned about the potential threat posed by that contractor's employees. Team members were also concerned about the lax behavior of many staff members at MedSite, especially regarding casual and loose conversations about patients. Smith acknowledged that the limitations of space and funding had resulted in extremely tight working conditions that virtually forced most admissions staff to share passwords

and accounts just to get their jobs done in a reasonable amount of time. Employees constituted a strong source of a range of accidental incidents.

With the exception of disgruntled employees, the team determined that the motivation of insiders was generally low (Step 14). Outsiders' motives were difficult to estimate, but the team did feel that being a small, relatively anonymous medical organization made MedSite a less attractive target for outsiders. The team decided that the motives of outsiders were low.

The team decided to talk to a few knowledgeable staff members at MedSite and ABC Systems to determine the known history for some of the threats (Step 15). ABC Systems had some data, but they were not comprehensive. In fact, given the lack of tangible data produced by people from ABC Systems, analysis team members became concerned about what ABC Systems was doing to monitor PIDS and other systems. The team member with information technology experience knew enough to be skeptical of ABC Systems' network monitoring practices. The team recorded a recommendation to the *Notes and Recommendations Worksheet* [p. 17] to verify what ABC Systems was doing to monitor MedSite's systems and networks. The team also marked its confidence in this historical data as low.

Specific areas of concern were recorded on the *Risk Profile Worksheets* (Step 16) [pp. 91 and 131] whenever the team had a particular example or historical incident relative to a threat. For example, it was well-known that staff members occasionally looked up patient information about their friends and relatives, violating privacy. In addition, the physical configuration of offices and the inclusion of workstations in patient rooms also led to many privacy violations. Alvarez mentioned that physicians were still having a hard time remembering to log off PIDS when they left a treatment room. All team members also noted PIDS' notorious history of failing at inopportune times. Finally, the team was concerned that ABC Systems did not really understand either the general needs of a medical facility or the effects of the new privacy and security regulations.

All actions items from Process S2 were documented on the *Action List Worksheet* [p. 27].

1.4.2 Phase 2: Identify Infrastructure Vulnerabilities

The analysis team met daily over the course of a few days to complete Phase 2. Team members performed a cursory examination of how people at MedSite accessed critical assets via the organization's networks. The team also reviewed the extent to which security was considered when configuring and maintaining MedSite's computers and networks. Because people at MedSite had little insight into what ABC Systems was doing to configure and maintain MedSite's systems and networks, the team decided to record a recommendation (see *Notes and Recommendations Worksheet* [p. 17]). The recommendation called for MedSite's IT staff to work

more closely with ABC Systems after the evaluation to communicate MedSite's security requirements to ABC Systems and to verify that those requirements were being met.

1.4.2.1 Process S3: Examine the Computing Infrastructure in Relation to Critical Assets

S3.1: Examine access paths (Steps 17 – 18)

The analysis team used the *Network Access Paths Worksheet* [p. 139] as it reviewed how people accessed MedSite's critical assets. The team noted that PIDS was its own system of interest (Step 17). It also noted that ECDS was its own system of interest, while PCs included all major systems as their systems of interest. Neither ABC Systems nor the paper medical records were reviewed during this phase, because network attacks are irrelevant to these types of assets.

For PIDS, the analysis team identified key classes of components that were part of or related to PIDS. This activity included a cursory examination of internal and external access points for PIDS (Step 18). Team members had different views of what constituted the PIDS system. After much discussion, they agreed that PIDS included server A and on-site workstations (Step 18a). They then looked at how people typically accessed PIDS. The team determined that people used on-site workstations, laptops, PDAs, and home workstations to access PIDS (Step 18c). The team decided that intermediate access points included both internal and external networks (Step 18b) and that PIDS information was stored both locally and off-site (Step 18d). Finally, the team determined that other systems, most notably ECDS and the Financial Record Keeping System (FRKS), also automatically accessed information from PIDS (Step 18e).

S3.2: Analyze technology-related processes (Steps 19 – 21)

This activity requires an analysis team to assume an infrastructure point of view when analyzing information. MedSite's team documented the key classes of components (Step 19a) and then noted which critical assets were related to each key class (Step 19b). The team then determined who was responsible for maintaining and securing each key class (Step 20). Where MedSite's own IT personnel were responsible for day-to-day operations, they could make an estimate of how secure the component classes were (Step 21). Many classes, however, were maintained by ABC Systems, and the level of security for those classes was unknown. The analysis team recorded this information on the *Infrastructure Review Worksheet* [p. 143].

Overall, the security of most classes of components was not consistently known. The team recorded some general recommendations to pursue the relationship with ABC Systems and work towards more formal vulnerability testing with them on the *Notes and Recommendations Worksheet* [p. 17].

Finally, the team reviewed the *Risk Profiles* for PIDS, ECDS, and PCs [pp. 91 and 131] as well as the *Security Practices Worksheet* [p. 51], looking to refine information on those worksheets based on the team's Phase 2 analysis. Team members decided there were no changes to the threat trees, just more validation for the concerns already identified. They did add an additional area of concern on the *Risk Profile Worksheet* (Step 16) [p. 131] about ABC Systems personnel not only having access to patient information but also being able to destroy it.

The IT team member also brought up the concern that what he observed on a daily basis did not support ABC Systems' statements that it kept up with vulnerability testing and patches. The team recorded this observation on the *Security Practices Worksheet* [p. 51] as an example of what MedSite's contractor was not doing well.

No other action items, notes, or recommendations from Process S3 were identified.

1.4.3 Phase 3: Develop Security Strategy and Plans

The analysis team added an additional team member to help with the development of mitigation plans in Process S5. The new team member had a lot of expertise in problem solving as well as developing plans, budgets, and schedules for MedSite. To ensure that she developed an understanding of the evaluation, the new team member observed Process S4.

1.4.3.1 Process S4: Identify and Analyze Risks

S4.1: Evaluate impact of threats (Step 22)

The analysis team used the *Impact Evaluation Criteria* [p. 33] they developed during Process S1 to evaluate the impacts of the threats on the organization. The team recorded all impact values on the *Risk Profile Worksheets* [pp. 91 and 131]. Team members considered the health and safety of patients to be the most important criteria, with the remaining criteria all being equal to each other. The team had some difficulty estimating the impacts to productivity and reputation for a few of the threats and decided to get additional help. Team members identified key people with experience in legal matters, public relations, and nursing to help the team estimate the values for certain threats. Together, they all reviewed each area of concern and talked about the types of specific actions that would have to be taken to deal with a realized threat, providing a basis for estimating the actual level of impact (high, medium, low). In particular, team members looked for any threats that might result in physical harm or death to patients. The team also noted on the *Notes and Recommendations Worksheet* [p. 17] that the evaluation criteria should be more broadly reviewed and approved by management.

S4.2: Establish probability evaluation criteria (Step 23)

The team defined MedSite's probability evaluation criteria using the *Probability Evaluation Criteria Worksheet* [p. 149]. It relied on its experience and expertise as well as the limited historical information it had for threats. Team members reviewed the known histories of threats recorded on the *Risk Profile Worksheets* [pp. 91 and 131] when setting probability measures (high, medium, low). When defining the criteria, the team also referenced historical data about certain types of threats commonly used by other medical organizations when assessing risk.

S4.3: Evaluate probabilities of threats (Step 24)

Using the *Probability Evaluation Criteria* [p. 149], the team evaluated the probability of each active threat occurring by using the contextual information they had previously recorded on the *Risk Profile Worksheets* (Steps 13-16) [pp. 91 and 131]. Because they had low confidence in their historical estimations for network-based threats, team members lacked confidence in their probability estimates for those types of threats. However, for a few threats, such as unauthorized insiders accidentally viewing information via systems and networks, team members were quite confident that the probability was high because of the known history of such actions. Because it had minimal confidence in many of its probability estimates, the team decided to use probability only as a tie-breaker when selecting risks for mitigation. Impact would be the primary decision-making driver. The team recorded estimates for probability for all active risks on the *Risk Profile Worksheets* [pp. 91 and 131].

No additional actions, notes, or recommendations were identified during Process S4.

1.4.3.2 Process S5: Develop Protection Strategy and Mitigation Plans

S5.1: Describe current protection strategy (Step 25)

The analysis team reviewed the *Security Practices Worksheet* [p. 51] that it completed earlier in the evaluation. Team members transcribed the stoplight status for each area to the *Protection Strategy Worksheets* [p. 153]. They then discussed the current practices and vulnerabilities identified in each practice area. The team noted that the protection strategy and the security practices survey examine two different facets of security practice areas. The protection strategy describes the processes used to perform activities in each security practice area, focusing on the extent to which processes are formally defined. On the other hand, the stoplight status on the security practices survey indicates how well the team believes its organization is performing in each area. Team members noted that an organization could be performing very well in an area, but have very informal processes. Likewise, an organization could have significant room for improvement despite having very formal policies and procedures. They defined the current protection strategy for the organization and recorded the results on the *Protection Strategy*

Worksheets [p. 153]. The protection strategy, along with stoplight status information, provided team members with a broad view of MedSite's overall approach to security and the extent to which it was working.

S5.2: Select mitigation approaches (Steps 26 - 27)

The team transcribed the stoplight statuses from the *Security Practices Worksheet* [p. 51] to the *Risk Profile Worksheets* (Step 26) [pp. 91 and 131], illustrating the current status of each security practice area in relation to the active risks. Before proceeding, the analysis team needed to agree upon the criteria for making decisions. Team members decided that they would look to mitigate risks meeting the following criteria:

- **risks affecting the health and safety of MedSite's patients (i.e., risks with a high impact value for the "Safety" impact area). Reputation and financial impacts were considered to be secondary factors.**
- **risks affecting the most important security requirement (Step 10) of the asset (e.g., availability of PIDS)**
- **risks linked to specific areas of concern about the asset**

Because it had little confidence in many if its probability estimates, the team decided to use probability as a tie-breaker when comparing two similar risks. Team members reviewed the *Risk Profile Worksheet* for each critical asset [pp. 91 and 131], focusing on potential impacts of risks in relation to stoplight statuses. The analysis team was initially overwhelmed. It had assigned nine security practice areas "red" stoplight statuses and six security practice areas "yellow" stoplight statuses. However, the team did not assign a "green" stoplight status to any area. Based on its decision-making criteria, the team looked across all critical assets and decided which risks it would mitigate. Next it decided which risks it could accept. All remaining risks were designated to be deferred and revisited at a later date. The analysis team decided to recommend (on the *Notes and Recommendations Worksheet* [p. 17]) that all deferred risks be looked at again a month after the end of the evaluation.

To mitigate the risks, the team selected the following security practice areas as mitigation areas:

- Security Awareness and Training **– The analysis team believed that their security awareness training did not adequately prepare personnel to handle the day-to-day security issues that arise. Improving this area should reduce the accidental, inside threat sources.**
- Collaborative Security Management **– ABC Systems provided support for managing the network and most of the systems at MedSite, including PIDS. ABC Systems also conducted periodic vulnerability evaluations of MedSite's computing infrastructure. The analysis team was concerned about MedSite's procedures for working with ABC**

Systems. The team believed that ABC Systems might not be meeting MedSite's information security requirements. Many unanswered questions and ambiguities arose during Process S3, so the team recommended that MedSite review and revise its procedures for working with ABC Systems. With respect to physical security, the Facilities Management Group was responsible for physically securing MedSite's building. No one at MedSite has been formally working with the staff from Facilities Management group. Because of this, the team recommended that the organization review and revise procedures for working with the Facilities Management Group.

- Monitoring and Auditing Physical Security **– There was some concern by team members that physical security problems existed at MedSite and were not being handled by the Facilities Management Group. The team identified several risks with potentially high impact to the health and safety of patients based on physical access by internal and external threat actors. The team decided that practices related to *Physical Access Control* were adequate. However, practices related to *Monitoring and Auditing Physical Security* required significant improvement. For this reason, *Monitoring and Auditing Physical Security* was selected as a mitigation area. However, because third parties were involved in monitoring and auditing physical security for MedSite, there was some overlap with the *Collaborative Security Management* security practice area.**
- Authentication and Authorization **– MedSite was not using a consistent means of controlling access to its systems and networks (e.g., role-based management of accounts). Staff members inherited far too many access privileges over time. The team was concerned about the potential consequences of these issues. For example, disgruntled staff members could abuse this increased access to affect the availability of PIDS or to modify medical information.**

The team documented its rationale for selecting each area on the *Notes and Recommendations Worksheet* [p. 17]. It also circled mitigation areas on the appropriate *Risk Profile Worksheets* [pp. 91 and 131] that reduce risks designated as "mitigate." Despite its own earlier recommendation to look at *Vulnerability Management* as a mitigation area, the team decided that the improvements in the *Collaborative Security Management* area could mitigate a greater number of risks related to the computing infrastructure than could improvements in *Vulnerability Management*.

S5.3: Develop risk mitigation plans (Step 28)

The team developed mitigation plans for each selected area using the *Mitigation Plan Worksheets* [p. 181]. The plan for each selected security practice area includes specific activities designed to mitigate specified risks. Some of the mitigation activities were quite broad in nature. For example, one mitigation activity indicated that periodic security awareness training should be provided for all employees once a year. Other mitigation activities were more focused in nature. For example, one mitigation activity specified that IT staff members receive training in particular technologies. This activity did not address training across all technologies, only for a selected

few. As it defined each mitigation activity, the team also recorded its rationale for that particular activity (what was it mitigating or improving), who should be responsible for the activity, and any additional management action that might be required to implement that activity.

S5.4: Identify changes to protection strategy (Step 29)

The analysis team reviewed the *Protection Strategy Worksheets* [p. 153] to note any changes triggered by mitigation activities. For example, the mitigation activity that called for security awareness training for all employees once a year triggered a change in MedSite's protection strategy. The protection strategy previously required security awareness training only for new employees. On the other hand, the mitigation activity that specified training in particular technologies for IT staff members did not trigger a change in MedSite's protection strategy because the activity did not address training for all technologies. This activity simply improved how one aspect of MedSite's protection strategy was implemented.

Next, the team reviewed the protection strategy, looking for any additional changes to the strategy that it wanted to make. It immediately focused on the *Security Policies and Regulations* area. MedSite had a partial set of documented security-related policies. Because MedSite would soon be required to comply with new data security regulations, the team decided that procedures for complying with those regulations would need to be created. It marked that change to the protection strategy. Team members also noted that while some security-related policies existed, few staff members understood them. Since security awareness training was already being updated, the team decided to include information about MedSite's security policy in that training. Finally, the team decided to address policy enforcement. Even if people knew about and understood MedSite's security policy, their behaviors would change only if they also knew that management was enforcing that policy. Thus, the team decided that procedures for enforcing MedSite's policy needed to be created. The team then developed a mitigation plan to implement the changes to the *Security Policies and Regulations* area. In the rationale area for each mitigation activity, the team noted that these activities were driven by general concerns and regulations, rather than by specific risks.

The analysis team also identified the following two action items during Process S5, documenting them on the *Action List Worksheet* [p. 27]:

- ***Resend basic security policy reminders.*** **The IT department had sent emails to all staff in the past regarding basic security policy issues. Because improving MedSite's security awareness and training program was seen as a long-term initiative, this action item provided a short-term awareness mechanism without much investment.**
- ***Change the physical configuration of the admissions office.*** **One of the physical security problems identified during the evaluation was the physical configuration of the admissions area. Most workstations were directed toward public areas, where patients**

and staff could see medical information on the screens of those workstations. To protect the privacy of medical and admissions information, the analysis team decided to recommend changing the configuration of the admissions office to ensure that workstations could not be easily seen by people passing through the admissions area.

S5.5: Identify next steps (Step 30)

Using the *Next Steps Worksheet* [p. 195], the team identified several items required to support implementation of OCTAVE-S results. First, senior management needed to make information security a priority and not a back-burner issue. Second, adequate funding to implement the mitigation plans, protection strategy changes, and action items needed to be allocated. The team also noted that the following items would need to be completed within the next month.

- **People who had been assigned responsibility for implementing a mitigation plan will provide a *detailed* implementation plan for review.**
- **All deferred risks will be reviewed.**
- **The analysis team will compare the security practice surveys to regulations (including HIPAA) to determine if there are any additional practices that need to be added or improved to comply with current regulations.**

The team also recommended conducting another OCTAVE-S evaluation in about 12-18 months, providing sufficient time to implement the recommendations from the evaluation it had just completed.

2 Notes and Recommendations Worksheet

Note	
What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
With no indications that we have been externally attacked, we don't know if the reason is that we really haven't been attacked or that no one is monitoring the right things to determine if we have been.	Step __12__

Note	
What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Recommendation

What recommendations do you want to record?	*For which step is this recommendation relevant?*
We need a way to determine what ABC Systems is doing to monitor for external attacks. This may require a contractual discussion.	Step __15___

Recommendation

What recommendations do you want to record?	*For which step is this recommendation relevant?*
We need a more formal or increased communication with ABC Systems.	Step __21___

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
We do not believe vulnerability management is being adequately performed on PIDS.	Step __21__

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Recommendation	
What recommendations do you want to record?	*For which step is this recommendation relevant?*
The ability to manage vulnerabilities should be a candidate for a risk mitigation plan in Phase 3. This may also be more of ABC Systems' responsibility than ours.	Step __27___

Recommendation	
What recommendations do you want to record?	*For which step is this recommendation relevant?*
Security Awareness and Training is selected as a mitigation area. Rationale: MedSite's security awareness training does not adequately address the security issues that staff members face on a daily basis. Improving this area would help to address several risks with a high safety impact linked to accidental actions by staff members.	Step __27___

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Note

What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Recommendation	
What recommendations do you want to record?	*For which step is this recommendation relevant?*
Collaborative Security Management is selected as a mitigation area. Rationale: ABC Systems provides support for managing the network and most of the systems at MedSite, including PIDS. ABC Systems also conducts periodic vulnerability evaluations of MedSite's computing infrastructure. ABC Systems might not be meeting MedSite's information security requirements. Since ABC Systems plays such a vital role in configuring, maintaining, and securing MedSite's computing infrastructure, procedures for working with ABC Systems should be reviewed and revised.	Step __27___

Recommendation	
What recommendations do you want to record?	*For which step is this recommendation relevant?*
Monitoring and Auditing Physical Security is selected as a mitigation area. Rationale: There is concern that physical security problems exist at MedSite. The team identified several risks with potentially high impact to the health and safety of patients based on physical access by internal and external threat actors. However, the team does not have enough information to determine exactly how to address the issue. Conducting a physical security audit will characterize the extent of the problem.	Step __27___

Note	
What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Note	
What notes do you want to record? *Is there a recommendation associated with this note? If yes, document it in the corresponding recommendations box.*	*For which step is this note relevant?*
	Step _____

Recommendation

What recommendations do you want to record?	*For which step is this recommendation relevant?*
Authentication and Authorization is selected as a mitigation area. Rationale: MedSite is currently not using role-based management of accounts. In addition, staff members inherit far too many access privileges over time. The team is concerned about the potential consequences of these issues. For example, disgruntled staff members could abuse this increased access to modify information.	Step __27___

Recommendation

What recommendations do you want to record?	*For which step is this recommendation relevant?*
Look at all deferred risks again in 30 days.	Step __26___

3 Action List Worksheet

Action Item

	What actions do you intend to take? *Assign an identification number to each action item.*	*For which step is this action item relevant?*
ID # 1	Ask ABC systems what other medical-related customers they have and if we could talk to them.	Step 13

Action Item

	What actions do you intend to take? *Assign an identification number to each action item.*	*For which step is this action item relevant?*
ID # 2	Look for other vendors in this vicinity who could be candidates for taking over our systems should we need an alternative vendor. Check medical conferences and society meetings/seminars.	Step 13

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?* Administration – contract manager
Completion Date:	*By when must the action item be completed?* Within the next 2 weeks
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?* Analysis team members and a few others who attend conferences and seminars.
Completion Date:	*By when must the action item be completed?* Within the next 6 months
Additional Support:	*What additional support (by management or others) is required to complete the action item?*

Action Item

ID #	*What actions do you intend to take?* *Assign an identification number to each action item.*	*For which step is this action item relevant?*
___3___	Resend basic security policy reminders.	Step __29___

Action Item

ID #	*What actions do you intend to take?* *Assign an identification number to each action item.*	*For which step is this action item relevant?*
___4___	Change the physical configuration of the admissions office.	Step __29___

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?* IT Group
Completion Date:	*By when must the action item be completed?* Within the next 2 weeks
Additional Support:	*What additional support (by management or others) is required to complete the action item?* MedSite's CIO needs to approve this action item and assign it to someone in the IT group.

	Action Item
	What additional information do you want to document for each action item? *Record additional information below.*
Responsibility:	*Who is responsible for completing the action item?* Facilities Management
Completion Date:	*By when must the action item be completed?* Within the next month
Additional Support:	*What additional support (by management or others) is required to complete the action item?* MedSite's management team needs to approve this action item and assign it to the Facilities Management Group.

4 Impact Evaluation Criteria Worksheet

Step 1

Step 1

Reputation/Customer Confidence

Impact Type	Low Impact
Reputation	Reputation is minimally effected; little or no effort or expense is required to recover.
Customer Loss	Less than __10__% reduction in customers due to loss of confidence
Other:	
Other:	

Reputation/Customer Confidence	
Medium Impact	**High Impact**
Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
__10__ to __30__% reduction in customers due to loss of confidence	More than __30__% reduction in customers due to loss of confidence

Step 1

Financial

Impact Type	Low Impact
Operating Costs	Increase of less than ___2___% in yearly operating costs
Revenue Loss	Less than ___5___% yearly revenue loss
One-Time Financial Loss	One-time financial cost of less than $__250,000__
Other:	

Financial	
Medium Impact	**High Impact**
Yearly operating costs increase by ___2___to __15___%	Yearly operating costs increase by more than __15___%
___5___to ___20__% yearly revenue loss	Greater than ___20__% yearly revenue loss
One-time financial cost of $__250,000__ to $_1 million __	One-time financial cost greater than $_1 million __

Step 1

Productivity

Impact Type	Low Impact
Staff Hours	Staff work hours are increased by less than __10__% for _____~~to~~ __2__ day(s).
Other:	
Other:	
Other:	

Productivity	
Medium Impact	**High Impact**
Staff work hours are increased between __10__% and __30__% for ~~———~~ to __2__ day(s).	Staff work hours are increased by greater than __30__% for ~~———~~ to __2__ day(s).

Step 1

Safety/Health

Impact Type	Low Impact
Life	patients' No loss or significant threat to ~~customers' or staff members'~~ lives
Health	Minimal, immediately treatable degradation in ~~customers' or staff members'~~ health with recovery within four days patients'
Safety	Safety questioned
Other:	

Safety/Health	
Medium Impact	**High Impact**
Patients' ~~Customers' or staff members'~~ lives are threatened, but they will recover after receiving medical treatment.	patients' Loss of ~~customers' or staff members'~~ lives
Temporary or recoverable impairment of ~~customers' or staff members'~~ health patients'	Permanent impairment of significant aspects of ~~customers' or staff members'~~ health patients'
Safety affected	Safety violated

Step 1

Fines/Legal Penalties

Impact Type	Low Impact
Fines	Fines less than $__10,000___ are levied.
Lawsuits	Non-frivolous lawsuit(s) less than $_100,000__ are filed against the organization or frivolous lawsuit(s) are filed against the organization.
Investigations	No queries from government or other investigative organizations.
Other:	

Fines/Legal Penalties

Medium Impact	High Impact
Fines between $__10,000___ and $_100,000__ are levied.	Fines greater than $_100,000__ are levied.
Non-frivolous lawsuit(s) between $_100,000__ and $_1 million __is filed against the organization.	Non-frivolous lawsuit(s) greater than $_1 million __is filed against the organization.
Government or other investigative organization requests information or records (low profile).	Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices.

5 Asset Identification Worksheet

Step 2

Step 2

Information, Systems, and Applications

System	**Information**
What systems do people in your organization need to perform their jobs?	*What information do people in your organization need to perform their jobs?*
Patient Information Data System (PIDS)	– patient medical information
Financial Record Keeping System (FRKS)	– billing records – insurance records – payment schedules
Emergency Care Data System (ECDS)	– billing records – insurance records
personal computers	– patient medical information – billing records – insurance records – payment schedules – providers' credentials (paper files)
email server (for general email)	– information in emails – patient information (exchanges among doctors)

	Information, Systems, and Applications
Applications and Services	**Other Assets**
What applications and services do people in your organization need to perform their jobs?	*What other assets are closely related to these assets?*
– database application – email – Internet connectivity	– paper medical records – Internet Service Provider
– database application – Internet connectivity	– Internet Service Provider
– Internet connectivity	– Internet Service Provider
• email – Internet connectivity	– PIDS – FRKS – ECDS – other functional systems – Internet Service Provider
	– PIDS – personal computers

Step 2

People

People	**Skills and Knowledge**
Which people have a special skill or knowledge that is vital to your organization and would be difficult to replace?	*What are their special skills or knowledge?*
External relations	A group of people who controls the release of patient medical information
ABC Systems	Group that manages all major changes, maintenance, and upkeep of all major systems
MTF help desk	PC technicians who troubleshoot PC problems for users
Mr. Smith	Senior IT staff member. He is the only on-site staff member with networking skills.

	People
Related Systems	**Related Assets**
Which systems do these people use?	*Which other assets do these people use (i.e., information, services or applications)?*
– PIDS	
– PIDS – FRKS – ECDS – network	
– PCs	

6 Security Practices Worksheet

Steps 3a, 3b, and 4

1. Security Awareness and Training

Step 3a

Statement	To what extent is this statement reflected in your organization?
Staff members understand their security roles and responsibilities. This is documented and verified.	Very Much Somewhat (Not At All) Don't Know
There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.	Very Much Somewhat (Not At All) Don't Know
Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.	Very Much Somewhat (Not At All) Don't Know
Staff members follow good security practice, such as • securing information for which they are responsible • not divulging sensitive information to others (resistance to social engineering) • having adequate ability to use information technology hardware and software • using good password practices • understanding and following security policies and regulations • recognizing and reporting incidents	Very Much Somewhat (Not At All) Don't Know

1. Security Awareness and Training

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
– We have training, guidance, regulations, and policies. – Awareness training is required to get an account.	– There is a lack of training for IT staff. – Awareness training is inadequate. – Staff does not understand security issues. – There is little understanding of security roles and responsibilities. – People share accounts and passwords.	☒ Red ❑ Yellow ❑ Green ❑ Not Applicable

2. Security Strategy

Step 3a

Statement	To what extent is this statement reflected in your organization?
The organization's business strategies routinely incorporate security considerations.	Very Much Somewhat (Not At All) Don't Know
Security strategies and policies take into consideration the organization's business strategies and goals.	Very Much Somewhat (Not At All) Don't Know
Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization.	Very Much (Somewhat) Not At All Don't Know

2. Security Strategy

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
	– Our current protection strategy is not effective. – Our security strategy lacks business sense. It is not proactive.	☒ Red ❑ Yellow ❑ Green ❑ Not Applicable

3. Security Management

Step 3a

Statement	To what extent is this statement reflected in your organization?
Management allocates sufficient funds and resources to information security activities.	Very Much (Somewhat) Not At All Don't Know
Security roles and responsibilities are defined for all staff in the organization.	Very Much (Somewhat) Not At All Don't Know
All staff at all levels of responsibility implement their assigned roles and responsibility for information security.	Very Much Somewhat (Not At All) Don't Know
There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides.	Very Much Somewhat (Not At All) Don't Know
The organization's hiring and termination practices for staff take information security issues into account.	Very Much (Somewhat) Not At All Don't Know
The organization manages information security risks, including • assessing risks to information security • taking steps to mitigate information security risks	Very Much Somewhat (Not At All) Don't Know
Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risks and vulnerability assessments).	Very Much Somewhat Not At All (Don't Know)

3. Security Management

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
– This risk evaluation is a step in the right direction.	– We have an inadequate budget for security. – Staff members are complacent about security.	☒ Red ❑ Yellow ❑ Green ❑ Not Applicable

4. Security Policies and Regulations

Step 3a

Statement	To what extent is this statement reflected in your organization?
The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated.	(Very Much) Somewhat Not At All Don't Know
There is a documented process for management of security policies, including • creation • administration (including periodic reviews and updates) • communication	Very Much (Somewhat) Not At All Don't Know
The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements.	Very Much (Somewhat) Not At All Don't Know
The organization uniformly enforces its security policies.	Very Much Somewhat (Not At All) Don't Know

4. Security Policies and Regulations

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
– Policies and procedures exist. – There are established incident-handling policies and procedures.	– There is poor communication of policies. – People don't always read and follow policies and procedures. – There is a lack of follow-up on reported violations. – We don't enforce our policies.	❑ Red ☒ Yellow ❑ Green ❑ Not Applicable

5. Collaborative Security Management

Step 3a

Statement	To what extent is this statement reflected in your organization?
The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including • protecting information belonging to other organizations • understanding the security polices and procedures of external organizations • ending access to information by terminated external personnel	Very Much (Somewhat) Not At All Don't Know
The organization documents information protection requirements and explicitly communicates them to all appropriate third parties.	Very Much Somewhat (Not At All) Don't Know
The organization has formal mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.	Very Much Somewhat (Not At All) Don't Know
The organization has policies and procedures for collaborating with all third-party organizations that • provide security awareness and training services • develop security policies for the organization • develop contingency plans for the organization	Very Much (Somewhat) Not At All Don't Know

5. Collaborative Security Management

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
	– We rely on more than ABC Systems to support our networks. – There is no single point of contact for the network. Things get confused sometimes. – MedSite does not communicate its security-related requirements for PIDS to ABC Systems.	☒ Red ❑ Yellow ❑ Green ❑ Not Applicable

6. Contingency Planning/Disaster Recovery

Step 3a

Statement	To what extent is this statement reflected in your organization?
An analysis of operations, applications, and data criticality has been performed.	(Very Much) Somewhat Not At All Don't Know
The organization has documented, reviewed, and tested • business continuity or emergency operation plans • disaster recovery plan(s) • contingency plan(s) for responding to emergencies	Very Much (Somewhat) Not At All Don't Know
The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.	Very Much (Somewhat) Not At All Don't Know
All staff are • aware of the contingency, disaster recovery, and business continuity plans • understand and are able to carry out their responsibilities	Very Much (Somewhat) Not At All Don't Know

6. Contingency Planning/Disaster Recovery

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
– We have disaster recovery plans for natural disasters and some emergencies.	– We don't have a business continuity plan. – We don't have disaster recovery plans for systems and networks. – We're not sure how much testing has been done of the plans we do have.	❑ Red ☒ Yellow ❑ Green ❑ Not Applicable

7. Physical Access Control

Step 3a

Statement	To what extent is this statement reflected in your organization?
If staff from your organization is responsible for this area:	
Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested.	(Very Much) Somewhat Not At All Don't Know
There are documented policies and procedures for managing visitors.	(Very Much) Somewhat Not At All Don't Know
There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.	Very Much (Somewhat) Not At All Don't Know
Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.	Very Much (Somewhat) Not At All Don't Know
If staff from a third party is responsible for this area:	
The organization's requirements for physical access control are formally communicated to all contractors and service providers that control physical access to the building and premises, work areas, IT hardware, and software media.	Very Much (Somewhat) Not At All Don't Know
The organization formally verifies that contractors and service providers have met the requirements for physical access control.	Very Much (Somewhat) Not At All Don't Know

7. Physical Access Control

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
– We are required to lock our offices at the end of the day. – Physical security for our computer room is good.	– Once sensitive information is printed and distributed, it is not properly controlled or handled. – Physical security is hampered by o location/distribution of PCs o need to share PCs o shared office space o sharing codes to cipher locks o multiple access points to rooms	❑ Red ☒ Yellow ❑ Green ❑ Not Applicable

8. Monitoring and Auditing Physical Security

Step 3a

Statement	To what extent is this statement reflected in your organization?
If staff from your organization is responsible for this area:	
Maintenance records are kept to document the repairs and modifications of a facility's physical components.	Very Much Somewhat **(Not At All)** Don't Know
An individual's or group's actions, with respect to all physically controlled media, can be accounted for.	Very Much Somewhat **(Not At All)** Don't Know
Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed.	Very Much Somewhat **(Not At All)** Don't Know
If staff from a third party is responsible for this area:	
The organization's requirements for monitoring physical security are formally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	Very Much **(Somewhat)** Not At All Don't Know
The organization formally verifies that contractors and service providers have met the requirements for monitoring physical security.	Very Much Somewhat Not At All **(Don't Know)**

8. Monitoring and Auditing Physical Security

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
	– Audit records are spotty. We're not sure that anyone reviews them.	☒ Red ❑ Yellow ❑ Green ❑ Not Applicable

9. System and Network Management

Step 3a

Statement	To what extent is this statement reflected in your organization?
If staff from your organization is responsible for this area:	
There are documented and tested security plan(s) for safeguarding the systems and networks.	Very Much Somewhat **(Not At All)** Don't Know
Sensitive information is protected by secure storage (e.g., backups stored off site, discard process for sensitive information).	**(Very Much)** Somewhat Not At All Don't Know
The integrity of installed software is regularly verified.	Very Much **(Somewhat)** Not At All Don't Know
All systems are up to date with respect to revisions, patches, and recommendations in security advisories.	Very Much **(Somewhat)** Not At All Don't Know
There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans.	Very Much **(Somewhat)** Not At All Don't Know
Changes to IT hardware and software are planned, controlled, and documented.	Very Much **(Somewhat)** Not At All Don't Know
IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. • Unique user identification is required for all information system users, including third-party users. • Default accounts and default passwords have been removed from systems.	Very Much **(Somewhat)** Not At All Don't Know
Only necessary services are running on systems – all unnecessary services have been removed.	Very Much Somewhat **(Not At All)** Don't Know
Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced.	Very Much **(Somewhat)** Not At All Don't Know
If staff from a third party is responsible for this area:	
The organization's security-related system and network management requirements are formally communicated to all contractors and service providers that maintain systems and networks.	Very Much **(Somewhat)** Not At All Don't Know
The organization formally verifies that contractors and service providers have met the requirements for security-related system and network management.	Very Much Somewhat **(Not At All)** Don't Know

9. System and Network Management

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
– ABC Systems has a security plan. – We force users to change their passwords regularly. – ABC Systems has reported very few intrusions. – Systems are well protected with passwords. – ABC Systems runs tools from their site.	– MedSite has no documented security plan. – We don't clean up inherited access rights very well. – We're not sure whether ABC Systems keeps up with security notices. – We haven't been trained in the use of the latest system administration tools.	❑ Red ☒ Yellow ❑ Green ❑ Not Applicable

10. Monitoring and Auditing IT Security

Step 3a

Statement	To what extent is this statement reflected in your organization?
If staff from your organization is responsible for this area: System and network monitoring and auditing tools are routinely used by the organization. Unusual activity is dealt with according to the appropriate policy or procedure.	Very Much (Somewhat) Not At All Don't Know
Firewall and other security components are periodically audited for compliance with policy.	Very Much (Somewhat) Not At All Don't Know
If staff from a third party is responsible for this area: The organization's requirements for monitoring information technology security are formally communicated to all contractors and service providers that monitor systems and networks.	Very Much (Somewhat) Not At All Don't Know
The organization formally verifies that contractors and service providers have met the requirements for monitoring information technology security.	Very Much Somewhat (Not At All) Don't Know

10. Monitoring and Auditing IT Security

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
– ABC Systems does all IT audits. – ABC Systems runs monitoring tools.	– ABC Systems does not report unusual activity to anyone here.	❑ Red ☒ Yellow ❑ Green ❑ Not Applicable

11. Authentication and Authorization

Step 3a

Statement	To what extent is this statement reflected in your organization?
If staff from your organization is responsible for this area:	
Appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services, and network connections.	Very Much Somewhat **(Not At All)** Don't Know
There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.	Very Much **(Somewhat)** Not At All Don't Know
Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner. Methods or mechanisms are periodically reviewed and verified.	Very Much Somewhat **(Not At All)** Don't Know
If staff from a third party is responsible for this area:	
The organization's requirements for controlling access to systems and information are formally communicated to all contractors and service providers that provide authentication and authorization services.	Very Much **(Somewhat)** Not At All Don't Know
The organization formally verifies that contractors and service providers have met the requirements for authentication and authorization.	Very Much Somewhat **(Not At All)** Don't Know

11. Authentication and Authorization

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
– There are policies and procedures for access and control permissions. – Systems are protected well using passwords.	– We're not using role-based management of accounts. – People inherit far too many privileges.	☒ Red ❑ Yellow ❑ Green ❑ Not Applicable

12. Vulnerability Management

Step 3a

Statement	To what extent is this statement reflected in your organization?			
If staff from your organization is responsible for this area: There is a documented set of procedures for managing vulnerabilities, including • selecting vulnerability evaluation tools, checklists, and scripts • keeping up to date with known vulnerability types and attack methods • reviewing sources of information on vulnerability announcements, security alerts, and notices • identifying infrastructure components to be evaluated • scheduling of vulnerability evaluations • interpreting and responding to the results • maintaining secure storage and disposition of vulnerability data	Very Much	Somewhat	Not At All	Don't Know
Vulnerability management procedures are followed and are periodically reviewed and updated.	Very Much	Somewhat	Not At All	Don't Know
Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.	Very Much	Somewhat	Not At All	Don't Know
If staff from a third party is responsible for this area: The organization's vulnerability management requirements are formally communicated to all contractors and service providers that manage technology vulnerabilities.	Very Much	Somewhat	(Not At All)	Don't Know
The organization formally verifies that contractors and service providers have met the requirements for vulnerability management.	Very Much	Somewhat	Not At All	(Don't Know)

12. Vulnerability Management

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
– ABC Systems does all vulnerability evaluation and management.	– We haven't received training about how to interpret vulnerability reports.	☒ Red ❑ Yellow ❑ Green ❑ Not Applicable

13. Encryption

Step 3a

Statement	To what extent is this statement reflected in your organization?
If staff from your organization is responsible for this area: Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g., data encryption, public key infrastructure, virtual private network technology).	Very Much Somewhat (Not At All) Don't Know
Encrypted protocols are used when remotely managing systems, routers, and firewalls.	Very Much Somewhat (Not At All) Don't Know
If staff from a third party is responsible for this area: The organization's requirements for protecting sensitive information are formally communicated to all contractors and service providers that provide encryption technologies.	Very Much Somewhat Not At All (Don't Know)
The organization formally verifies that contractors and service providers have met the requirements for implementing encryption technologies.	Very Much Somewhat Not At All (Don't Know)

13. Encryption

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
	– We don't protect patient information when we send it electronically to third parties. – We don't know whether ABC Systems protects patient information using encryption. The topic has never come up.	☒ Red ❑ Yellow ❑ Green ❑ Not Applicable

14. Security Architecture and Design

Step 3a

Statement	To what extent is this statement reflected in your organization?
If staff from your organization is responsible for this area: System architecture and design for new and revised systems include considerations for • security strategies, policies, and procedures • history of security compromises • results of security risk assessments	Very Much Somewhat (Not At All) Don't Know
The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.	Very Much (Somewhat) Not At All Don't Know
If staff from a third party is responsible for this area: The organization's security-related requirements are formally communicated to all contractors and service providers that design systems and networks.	Very Much Somewhat (Not At All) Don't Know
The organization formally verifies that contractors and service providers have met the requirements for security architecture and design.	Very Much Somewhat (Not At All) Don't Know

14. Security Architecture and Design

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
	– PIDS II is being developed and no one has talked to us about security.	☒ Red ❑ Yellow ❑ Green ❑ Not Applicable

15. Incident Management

Step 3a

Statement	To what extent is this statement reflected in your organization?
If staff from your organization is responsible for this area: Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations.	Very Much (Somewhat) Not At All Don't Know
Incident management procedures are periodically tested, verified, and updated.	Very Much Somewhat (Not At All) Don't Know
There are documented policies and procedures for working with law enforcement agencies.	Very Much Somewhat (Not At All) Don't Know
If staff from a third party is responsible for this area: The organization's requirements for managing incidents are formally communicated to all contractors and service providers that provide incident management services.	Very Much Somewhat Not At All (Don't Know)
The organization formally verifies that contractors and service providers have met the requirements for managing incidents.	Very Much Somewhat Not At All (Don't Know)

15. Incident Management

Step 3b		Step 4
What is your organization currently doing well in this area?	**What is your organization currently *not* doing well in this area?**	**How effectively is your organization implementing the practices in this area?**
– Procedures exist for incident response.	– We have never considered how to deal with law enforcement. – It is not clear how or where we should report incidents. – We have never discussed incident management with ABC Systems.	❑ Red ☒ Yellow ❑ Green ❑ Not Applicable

7 Critical Asset Selection Worksheet

Step 5

Step 5

Questions to Consider:	*Which assets will have a large adverse impact on the organization if* • *they are disclosed to unauthorized people?* • *they are modified without authorization?* • *they are lost or destroyed?* • *access to them is interrupted?*

Critical Asset
1. Patient Information Data System (PIDS)
2. Paper medical records
3. Personal computers
4. ABC Systems
5. Emergency Data Care System (ECDS)

Notes
We are dependent on PIDS.
The number one data source for patient information is paper medical records.
All staff access key medical systems using personal computers.
They control our network.
This is typical of the 32 functional systems at MedSite.

8 Critical Asset Information Worksheet for Systems

Steps 6, 7, 8, 9, 10, and 11

Note that from this point on, most of the case scenario results are only for the critical asset PIDS.

Step 6 | **Step 7**

Critical Asset	**Rationale for Selection**
What is the critical system?	*Why is this system critical to the organization?*
Patient Information Data System (PIDS)	We are 98% dependent on PIDS for delivering patient care.

Step 9

Related Assets

Which assets are related to this system?

Information:

- Patient medical information

Services and Applications:

- Database
- Email

Other:

- Personal computers
- Paper medical records
- Internet connectivity
- ABC Systems
- External relations

Step 8

Description

Who uses the system? *Who is responsible for the system?*

Providers, lab technician, pharmacists, and appointment schedulers all use PIDS. Each group is responsible for a subset of the medical information on PIDS. ABC Systems has primary responsibility for maintaining PIDS. Some day-to-day maintenance work is performed by our IT staff.

Step 10

Security Requirements

What are the security requirements for this system?

(Hint: Focus on what the security requirements should be for this system, not what they currently are.)

☒ Confidentiality — Only authorized personnel can view information on ____PIDS_____. Information should be restricted to those with a "need to know." Information is subject to the privacy act.

☒ Integrity — Only authorized personnel can modify information on ____PIDS_____. Records must be complete and correct.

☒ Availability — _____PIDS____ must be available for personnel to perform their jobs. Access to information is required 24/7.

~~Unavailability cannot exceed _____ hour(s) per every _____ hours.~~

❑ Other — _____

_____

Step 11

Most Important Security Requirement

Which security requirement is most important for this system?

❑ Confidentiality

❑ Integrity

☒ Availability

❑ Other

9 Risk Profile Worksheets for Systems – PIDS

Steps 12, 13, 14, 15, 16, 22, 23, 24, 26, 27

9.1 Risk Profile Worksheet for PIDS – Human Actors Using Network Access

Human Actors Using Network Access | **Basic Risk Profile**

Step 12

Threat

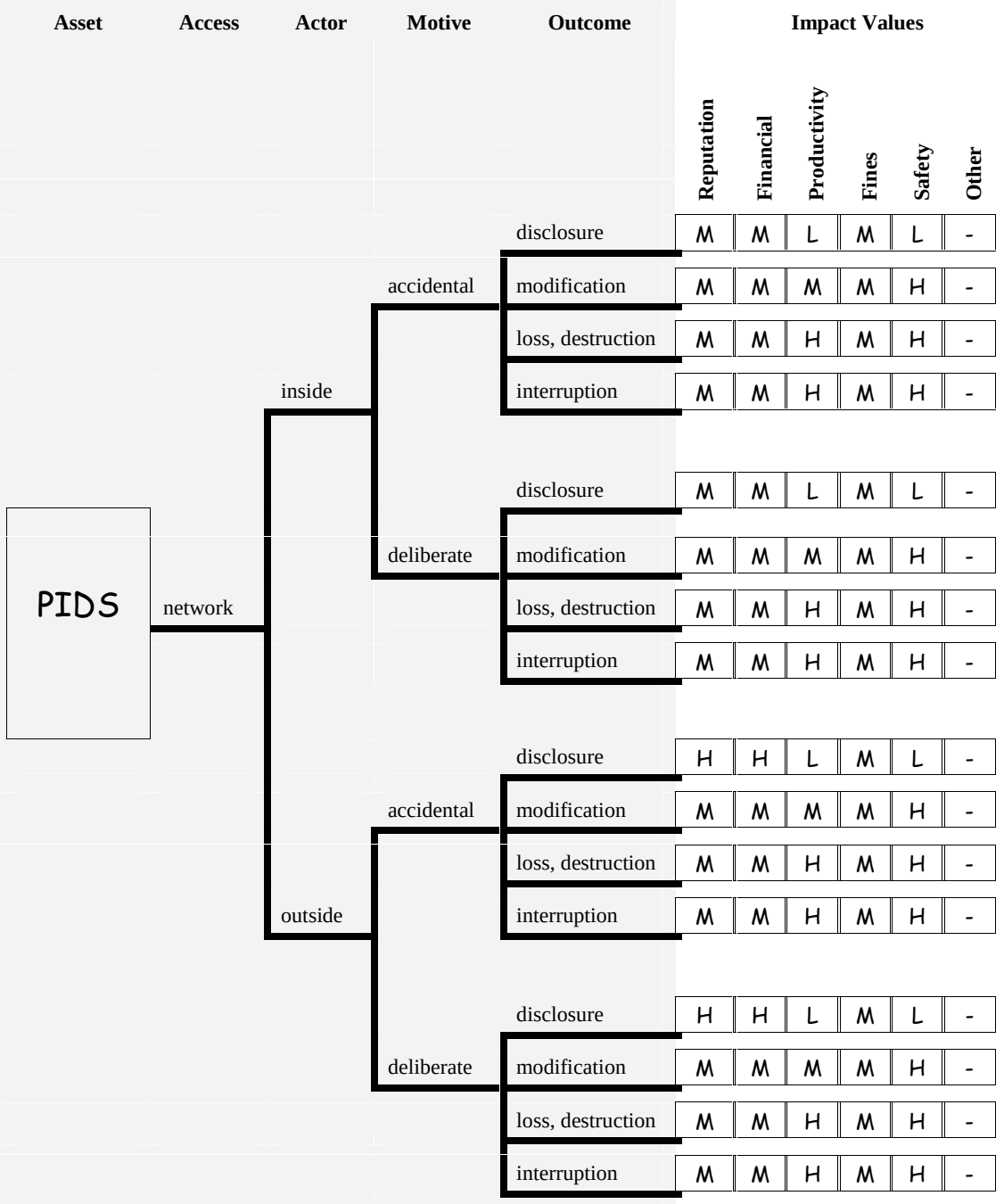
For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Step 22

Impact Values

What is the potential impact on the organization in each applicable area?



Basic Risk Profile — **Human Actors Using Network Access**

Step 24 — **Probability**

How likely is the threat to occur in the future? How confident are you in your estimate?

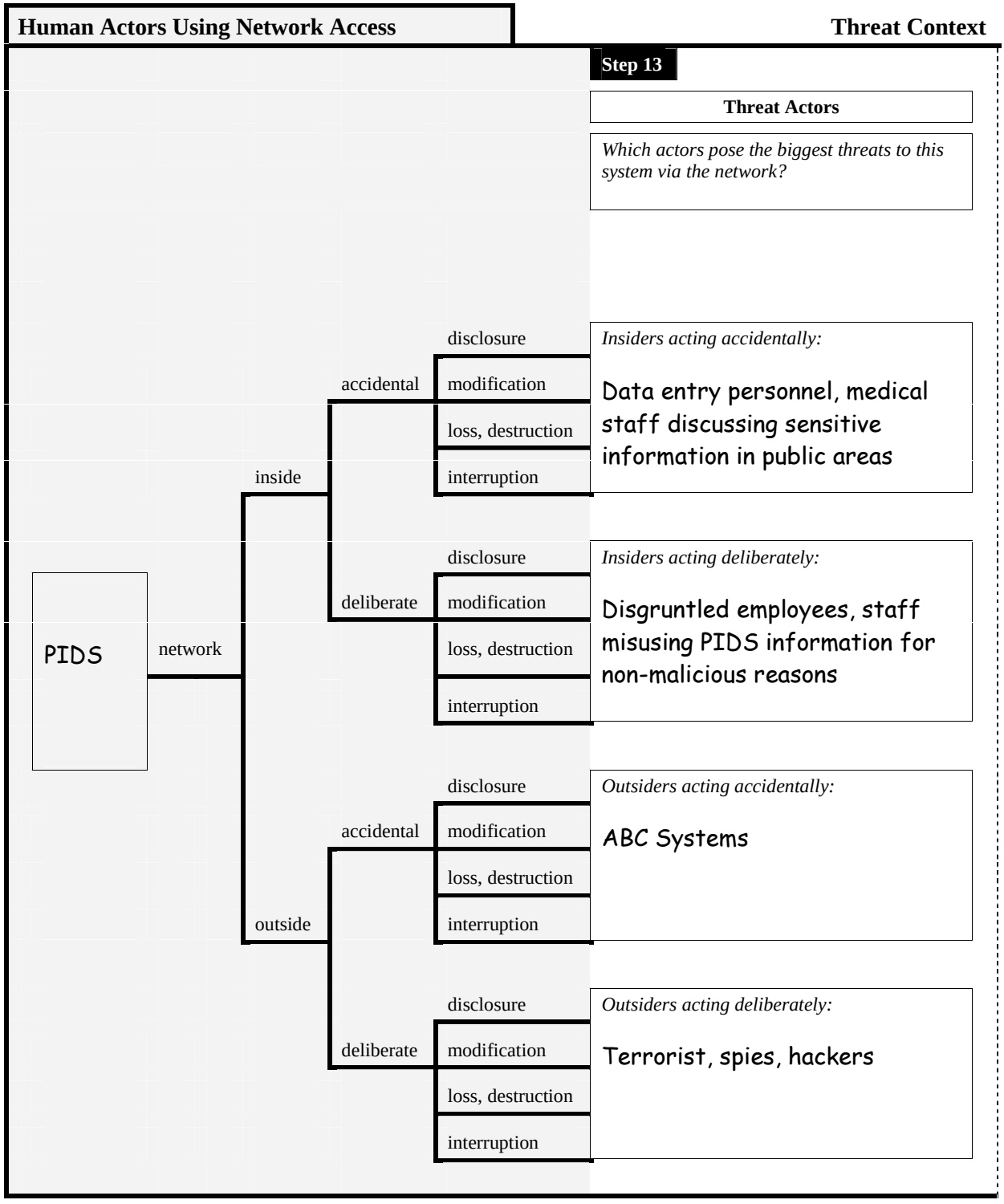
Step 26 — **Security Practice Areas**

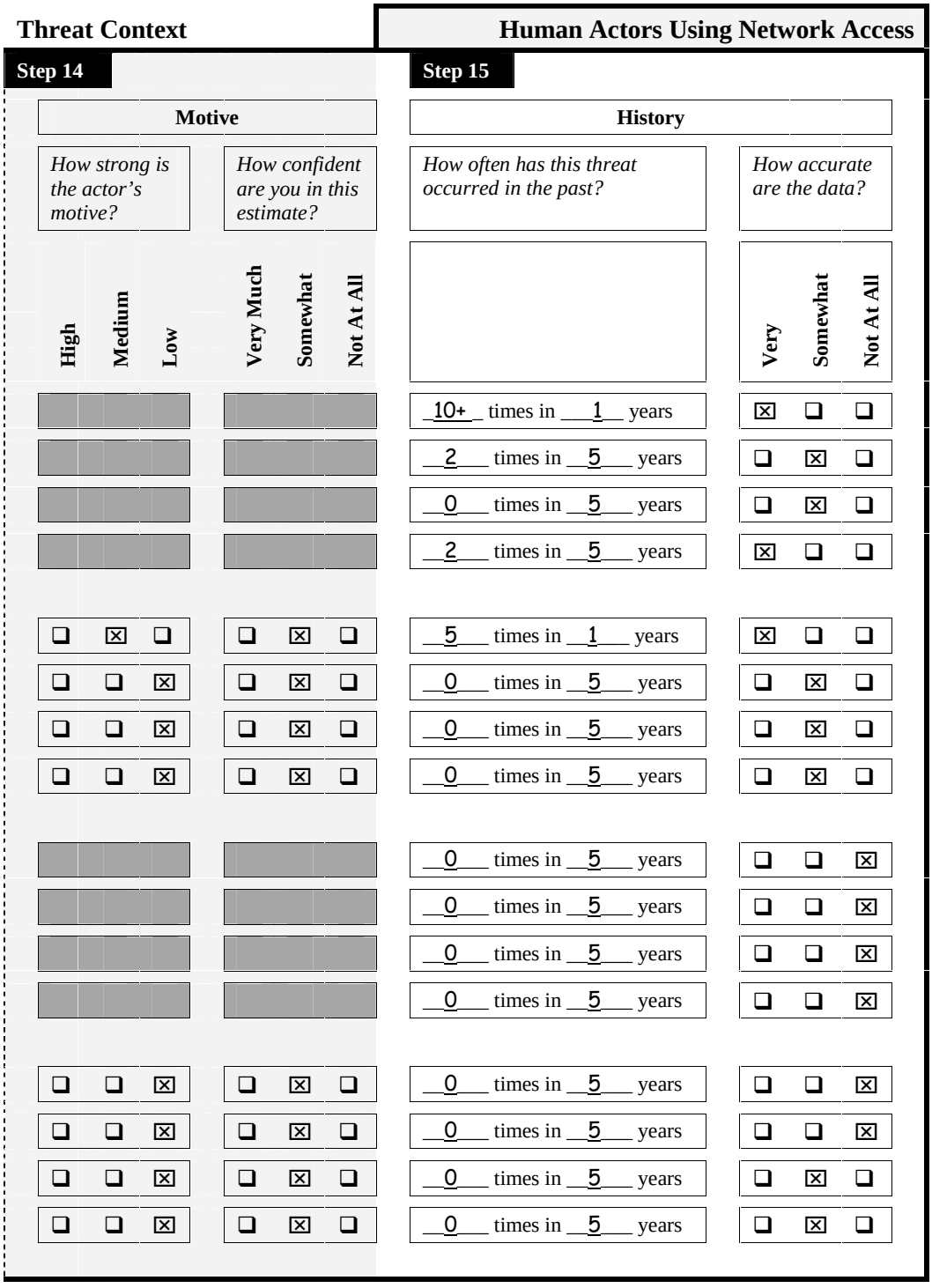
What is the stoplight status for each security practice area?

Step 27 — **Approach**

What is your approach for addressing each risk?

Value	Confidence	Strategic						Operational									Approach		
	Very Much / Somewhat / Not At All	1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt	Accept	Defer	Mitigate
H	|X----|------|	R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y	❑	☒	❑
L	|----X|------|	R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y	❑	☒	❑
L	|----X|------|	R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y	❑	☒	❑
L	|X----|------|	R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y	❑	☒	❑
H	|X----|------|	R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y	❑	❑	☒
L	|----X|------|	R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y	❑	❑	☒
L	|----X|------|	R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y	❑	❑	☒
L	|----X|------|	R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y	❑	❑	☒
L	|------|----X|	R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y	❑	☒	❑
L	|------|----X|	R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y	❑	☒	❑
L	|------|----X|	R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y	❑	☒	❑
L	|------|----X|	R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y	❑	☒	❑
L	|------|----X|	R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y	❑	❑	☒
L	|------|----X|	R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y	❑	❑	☒
L	|----X|------|	R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y	❑	❑	☒
L	|----X|------|	R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y	❑	❑	☒


Human Actors Using Network Access
Threat Context
Step 13
Threat Actors
Which actors pose the biggest threats to this system via the network?
PIDS
network
inside
outside
accidental
deliberate
disclosure
modification
loss, destruction
interruption
Insiders acting accidentally:
Data entry personnel, medical staff discussing sensitive information in public areas
Insiders acting deliberately:
Disgruntled employees, staff misusing PIDS information for non-malicious reasons
Outsiders acting accidentally:
ABC Systems
Outsiders acting deliberately:
Terrorist, spies, hackers



Threat Context | **Human Actors Using Network Access**

Step 14 | **Step 15**

Motive						History			
How strong is the actor's motive?			*How confident are you in this estimate?*			*How often has this threat occurred in the past?*	*How accurate are the data?*		
High	**Medium**	**Low**	**Very Much**	**Somewhat**	**Not At All**		**Very**	**Somewhat**	**Not At All**
						_10+_ times in ___1__ years	☒	❑	❑
						__2___ times in __5___ years	❑	☒	❑
						__0___ times in __5___ years	❑	☒	❑
						__2___ times in __5___ years	☒	❑	❑
❑	☒	❑	❑	☒	❑	__5___ times in __1___ years	☒	❑	❑
❑	❑	☒	❑	☒	❑	__0___ times in __5___ years	❑	☒	❑
❑	❑	☒	❑	☒	❑	__0___ times in __5___ years	❑	☒	❑
❑	❑	☒	❑	☒	❑	__0___ times in __5___ years	❑	☒	❑
						__0___ times in __5___ years	❑	❑	☒
						__0___ times in __5___ years	❑	❑	☒
						__0___ times in __5___ years	❑	❑	☒
						__0___ times in __5___ years	❑	❑	☒
❑	❑	☒	❑	☒	❑	__0___ times in __5___ years	❑	❑	☒
❑	❑	☒	❑	☒	❑	__0___ times in __5___ years	❑	❑	☒
❑	❑	☒	❑	☒	❑	__0___ times in __5___ years	❑	☒	❑
❑	❑	☒	❑	☒	❑	__0___ times in __5___ years	❑	☒	❑

Step 16

Human Actors Using Network Access	Areas of Concern
Insiders Using Network Access	
Give examples of how *insiders acting accidentally* could use network access to threaten this system.	
Give examples of how *insiders acting deliberately* could use network access to threaten this system.	Staff members with legitimate access to PIDS sometimes use that access to view information that they shouldn't (e.g., medical records of friends). This is a violation of the privacy act.
	Disgruntled employees are a concern. The more they know about information technology, the more dangerous they are.
Outsiders Using Network Access	
Give examples of how *outsiders acting accidentally* could use network access to threaten this system.	ABC Systems has access to PIDS and the network. Any deliberate or accidental acts by their staff could affect our ability to provide patient care.
Give examples of how *outsiders acting deliberately* could use network access to threaten this system.	Terrorists and spies are of concern. If they disrupt PIDS, they could shut down MedSite.
	Hackers are also a concern. If they disrupt PIDS, they could shut down MedSite.

Areas of Concern

Insiders Using Network Access
Role-based access builds over time. Many staff members have access to too much information.

Outsiders Using Network Access
ABC Systems has access to PIDS and the network. Any deliberate or accidental acts by their staff could affect our ability to provide patient care if they modify or delete vital information on PIDS.

9.2 Risk Profile Worksheet for PIDS – Human Actors Using Physical Access

Human Actors Using Physical Access — **Basic Risk Profile**

Step 12

Threat

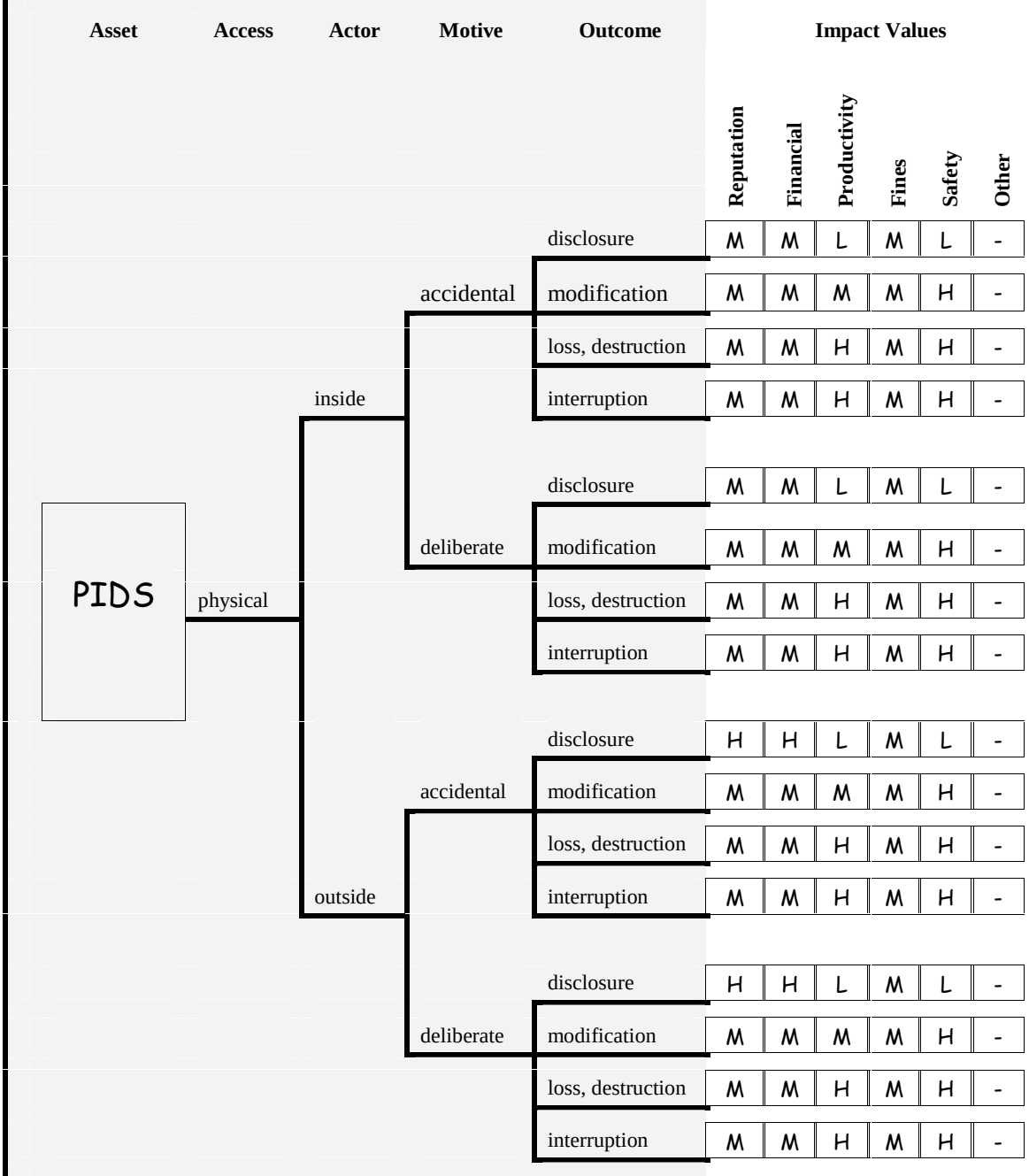
For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Step 22

Impact Values

What is the potential impact on the organization in each applicable area?



Basic Risk Profile — **Human Actors Using Physical Access**

Step 24 — **Probability**

How likely is the threat to occur in the future? How confident are you in your estimate?

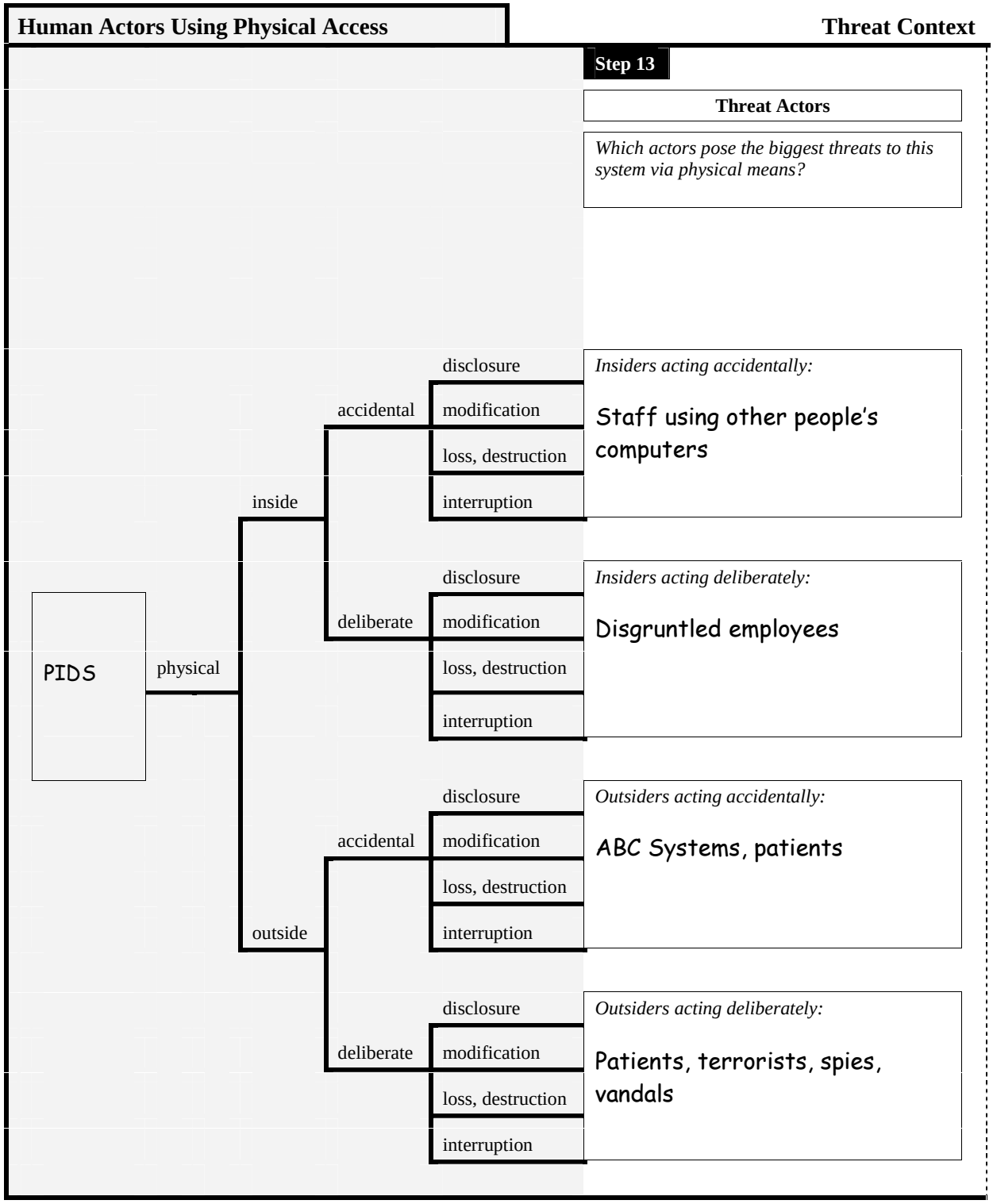
Step 26 — **Security Practice Areas**

What is the stoplight status for each security practice area?

Step 27 — **Approach**

What is your approach for addressing each risk?

Value	Confidence	Strategic						Operational									Approach		
	Very Somewhat Not At All	1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt	Accept	Defer	Mitigate
L	|----X|------|	R	R	R	Y	R	Y	Y	R						R	Y	❑	☒	❑
L	|----X|------|	R	R	R	Y	R	Y	Y	R						R	Y	❑	☒	❑
L	|----X|------|	R	R	R	Y	R	Y	Y	R						R	Y	❑	☒	❑
L	|----X|------|	R	R	R	Y	R	Y	Y	R						R	Y	❑	☒	❑
L	|----X|------|	R	R	R	Y	R	Y	Y	R						R	Y	❑	☒	❑
L	|----X|------|	R	R	R	Y	R	Y	Y	R						R	Y	❑	❑	☒
L	|----X|------|	R	R	R	Y	R	Y	Y	R						R	Y	❑	❑	☒
L	|----X|------|	R	R	R	Y	R	Y	Y	R						R	Y	❑	❑	☒
L	|------|----X|	R	R	R	Y	R	Y	Y	R						R	Y	❑	☒	❑
L	|------|----X|	R	R	R	Y	R	Y	Y	R						R	Y	❑	☒	❑
L	|------|----X|	R	R	R	Y	R	Y	Y	R						R	Y	❑	☒	❑
L	|------|----X|	R	R	R	Y	R	Y	Y	R						R	Y	❑	☒	❑
L	|----X|------|	R	R	R	Y	R	Y	Y	R						R	Y	❑	❑	☒
L	|----X|------|	R	R	R	Y	R	Y	Y	R						R	Y	❑	❑	☒
L	|----X|------|	R	R	R	Y	R	Y	Y	R						R	Y	❑	❑	☒
L	|----X|------|	R	R	R	Y	R	Y	Y	R						R	Y	❑	❑	☒


Human Actors Using Physical Access
Threat Context
Step 13
Threat Actors
Which actors pose the biggest threats to this system via physical means?
PIDS
physical
inside
outside
accidental
deliberate
disclosure
modification
loss, destruction
interruption
Insiders acting accidentally:
Staff using other people's computers
Insiders acting deliberately:
Disgruntled employees
Outsiders acting accidentally:
ABC Systems, patients
Outsiders acting deliberately:
Patients, terrorists, spies, vandals

Threat Context | **Human Actors Using Physical Access**

Step 14 | **Step 15**

Motive						History			
How strong is the actor's motive?			*How confident are you in this estimate?*			*How often has this threat occurred in the past?*	*How accurate are the data?*		
High	**Medium**	**Low**	**Very**	**Somewhat**	**Not At All**		**Very**	**Somewhat**	**Not At All**
						__2__ times in __5__ years	❑	☒	❑
						__0__ times in __5__ years	❑	☒	❑
						__0__ times in __5__ years	❑	☒	❑
						__0__ times in __5__ years	❑	☒	❑
❑	☒	❑	❑	☒	❑	__0__ times in __5__ years	❑	❑	☒
❑	❑	☒	❑	☒	❑	__0__ times in __5__ years	❑	❑	☒
❑	❑	☒	❑	☒	❑	__2__ times in __5__ years	❑	❑	☒
❑	❑	☒	❑	☒	❑	__0__ times in __5__ years	❑	❑	☒
						__0__ times in __5__ years	❑	❑	☒
						__0__ times in __5__ years	❑	❑	☒
						__0__ times in __5__ years	❑	❑	☒
						__0__ times in __5__ years	❑	❑	☒
❑	❑	☒	❑	☒	❑	__0__ times in __5__ years	❑	☒	❑
❑	❑	☒	❑	☒	❑	__0__ times in __5__ years	❑	☒	❑
❑	❑	☒	❑	☒	❑	__1__ times in __5__ years	❑	☒	❑
❑	❑	☒	❑	☒	❑	__0__ times in __5__ years	❑	☒	❑

Step 16

Human Actors Using Physical Access	Areas of Concern

Insiders Using Physical Access

Give examples of how *insiders acting accidentally* could use physical access to threaten this system.	
Give examples of how *insiders acting deliberately* could use physical access to threaten this system.	Any staff member can get physical access to PIDS by using PCs left unattended in exam rooms. PCs in exam rooms are typically left logged on to PIDS.
	Our main computer room is often left unlocked. Also, too many staff members seem to have keys to the room. Any staff member with malicious intent could gain access.

Outsiders Using Physical Access

Give examples of how *outsiders acting accidentally* could use physical access to threaten this system.	Any patient could accidentally see PIDS information when they are left alone in exam rooms. They could also deliberately look at PIDS information if they wanted to.
	ABC Systems has physical access all of our IT equipment. Any deliberate or accidental acts by their staff could affect our ability to provide patient care.
Give examples of how *outsiders acting deliberately* could use physical access to threaten this system.	Any patient could accidentally see PIDS information when they are left alone in exam rooms. They could also deliberately look at PIDS information if they wanted to.
	ABC Systems has physical access all of our IT equipment. Any deliberate or accidental acts by their staff could affect our ability to provide patient care.

Areas of Concern

Insiders Using Physical Access

Outsiders Using Physical Access
Terrorists and spies could attempt to physically access PIDS just as easily as they could try to hack it. If they disrupt PIDS, they could shut down MedSite.
The PIDS server is located at ABC Systems' site. Its staff has physical access to PIDS. Their physical security for the server is a concern.

9.3 Risk Profile Worksheet for PIDS – System Problems

System Problems | **Basic Risk Profile**

Step 12 | **Step 22**

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Impact Values

What is the potential impact on the organization in each applicable area?

Asset	Actor	Outcome	Impact Values					
			Reputation	Financial	Productivity	Fines	Safety	Other
PIDS	software defects	disclosure						
		modification						
		loss, destruction	M	M	H	M	H	-
		interruption	M	M	H	M	H	-
	system crashes	disclosure						
		modification						
		loss, destruction	M	M	H	M	H	-
		interruption	M	M	H	M	H	-
	hardware defects	disclosure						
		modification						
		loss, destruction	M	M	H	M	H	-
		interruption	M	M	H	M	H	-
	malicious code (virus, worm, Trojan horse, back door)	disclosure	H	H	L	M	L	-
		modification	M	M	M	M	H	-
		loss, destruction	M	M	H	M	H	-
		interruption	M	M	H	M	H	-

Basic Risk Profile — **Systems Problems**

Step 24

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value	Confidence (Very | Somewhat | Not At All)
	|------|------|
	|------|------|
H	|----X|------|
H	|X----|------|
	|------|------|
	|------|------|
H	|----X|------|
H	|X----|------|
	|------|------|
	|------|------|
L	|X----|------|
L	|X----|------|
L	|------|----X|
L	|------|----X|
L	|----X|------|
M	|----X|------|

Step 26

Security Practice Areas

What is the stoplight status for each security practice area?

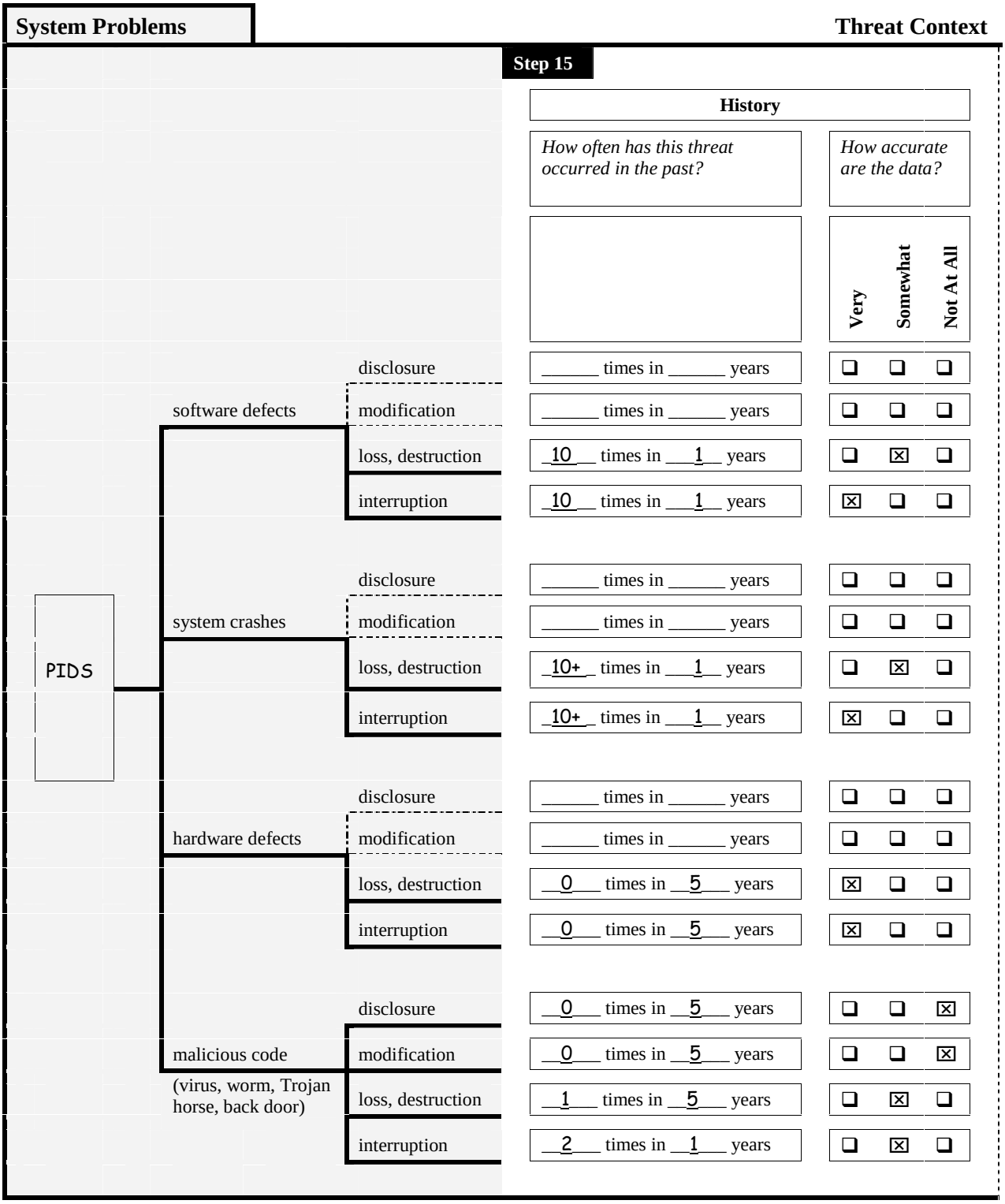
Strategic						Operational								
1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt
R	R	R	Y	R	Y			Y	Y		R		R	Y
R	R	R	Y	R	Y			Y	Y		R		R	Y
R	R	R	Y	R	Y			Y	Y	R	R		R	Y
R	R	R	Y	R	Y			Y	Y	R	R		R	Y
R	R	R	Y	R	Y			Y	Y		R		R	Y
R	R	R	Y	R	Y			Y	Y		R		R	Y
R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y
R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y
R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y
R	R	R	Y	R	Y			Y	Y	R	R	R	R	Y

Step 27

Approach

What is your approach for addressing each risk?

Accept	Defer	Mitigate
❑	❑	❑
❑	❑	❑
❑	☒	❑
❑	☒	❑
❑	❑	❑
❑	❑	❑
❑	☒	❑
❑	☒	❑
❑	❑	❑
❑	❑	❑
❑	☒	❑
❑	☒	❑
❑	☒	❑
❑	☒	❑
❑	☒	❑
❑	☒	❑


System Problems
Threat Context
Step 15
History
How often has this threat occurred in the past?
How accurate are the data?
Very
Somewhat
Not At All
PIDS
software defects
system crashes
hardware defects
malicious code
(virus, worm, Trojan horse, back door)
disclosure
modification
loss, destruction
interruption
_____ times in _____ years
_10__ times in ___1__ years
_10+_ times in ___1__ years
__0___ times in __5___ years
__1___ times in __5___ years
__2___ times in __1___ years

Threat Context | **System Problems**

Notes
What additional notes about each threat do you want to record?

Step 16

System Problems	Areas of Concern
Software Defects	
Give examples of how *software defects* could threaten this system.	The PIDS database application locks up periodically. To get PIDS back up, we need to reboot the system. Anytime PIDS is down, it affects MedSite's ability to provide patient care.
System Crashes	
Give examples of how *system crashes* could threaten this system.	PIDS has a history of crashing for a variety of reasons. Anytime PIDS is down, it affects MedSite's ability to provide patient care.
Hardware Defects	
Give examples of how *hardware defects* could threaten this system.	
Malicious Code	
Give examples of how *malicious code* could threaten this system. (Consider viruses, worms, Trojan horses, back doors, others)	Any vulnerability could be exploited by a virus or other type of malicious code.

Areas of Concern

Software Defects
System Crashes
Hardware Defects
Malicious Code
Viruses are a major concern. PIDS was shut down twice last year because of virus problems.

9.4 Risk Profile Worksheet for PIDS – Other Problems

Other Problems **Basic Risk Profile**

Step 12 **Step 22**

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Impact Values

What is the potential impact on the organization in each applicable area?

Asset	Actor	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other
PIDS	power supply problems	disclosure						
		modification						
		loss, destruction	M	M	H	M	H	-
		interruption	M	M	H	M	H	-
	telecommunications problems or unavailability	disclosure						
		modification						
		loss, destruction						
		interruption	M	M	H	M	H	-
	third-party problems or unavailability of third-party systems	disclosure						
		modification						
		loss, destruction						
		interruption	M	M	H	M	H	-
	natural disasters (e.g., flood, fire, tornado)	disclosure	H	H	L	M	L	-
		modification						
		loss, destruction	M	M	H	M	H	-
		interruption	M	M	H	M	H	-

Basic Risk Profile | **Other Problems**

Step 24 | **Step 26** | **Step 27**

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Security Practice Areas

What is the stoplight status for each security practice area?

Approach

What is your approach for addressing each risk?

Value	Confidence				Strategic						Operational									Approach		
	Very	Somewhat	Not At All		1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt	Accept	Defer	Mitigate
				|------|------|																❑	❑	❑
				|------|------|																❑	❑	❑
M		X		|----X|------|	R	R	R	Y	R	Y	Y	R							Y	❑	☒	❑
M	X			|X----|------|	R	R	R	Y	R	Y	Y	R							Y	❑	☒	❑
				|------|------|																❑	❑	❑
				|------|------|																❑	❑	❑
				|------|------|																❑	❑	❑
L	X			|X----|------|	R	R	R	Y	R	Y	Y	R							Y	❑	☒	❑
				|------|------|																❑	❑	❑
				|------|------|																❑	❑	❑
				|------|------|																❑	❑	❑
M	X			|X----|------|	R	R	R	Y	R	Y									Y	❑	❑	☒
L	X			|X----|------|	R	R	R	Y	R	Y	Y	R								❑	☒	❑
				|------|------|																❑	☒	❑
L	X			|X----|------|	R	R	R	Y	R	Y	Y	R								❑	☒	❑
L	X			|X----|------|	R	R	R	Y	R	Y	Y	R								❑	☒	❑

Other Problems — **Threat Context**

Step 15

			History			
			How often has this threat occurred in the past?	*How accurate are the data?*		
				Very	**Somewhat**	**Not At All**
PIDS	power supply problems	disclosure	_____ times in _____ years	❑	❑	❑
		modification	_____ times in _____ years	❑	❑	❑
		loss, destruction	__2__ times in __1__ years	❑	☒	❑
		interruption	__2__ times in __1__ years	☒	❑	❑
	telecommunications problems or unavailability	disclosure	_____ times in _____ years	❑	❑	❑
		modification	_____ times in _____ years	❑	❑	❑
		loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	__1__ times in __5__ years	☒	❑	❑
	third-party problems or unavailability of third-party systems	disclosure	_____ times in _____ years	❑	❑	❑
		modification	_____ times in _____ years	❑	❑	❑
		loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	__3__ times in __2__ years	☒	❑	❑
	natural disasters (e.g., flood, fire, tornado)	disclosure	__0__ times in __5__ years	☒	❑	❑
		modification	_____ times in _____ years	❑	❑	❑
		loss, destruction	__2__ times in __5__ years	☒	❑	❑
		interruption	__2__ times in __5__ years	☒	❑	❑

Threat Context | **Other Problems**

Notes
What additional notes about each threat do you want to record?
Power supply is controlled by the site and its facilities group.

Step 16

Other Problems	Areas of Concern
Power Supply Problems	
Give examples of how *power supply problems* could threaten this system.	Power supply problems can lead to a denial of access to PIDS. Our backup procedures have failed in the past, so this is a concern.
Telecommunications Problems	
Give examples of how *telecommunications problems* could threaten this system.	We access PIDS using telecommunications lines. If there is a problem with any telecommunications equipment, then we could not access PIDS.
Third-Party Problems	
Give examples of how *third-party problems* could threaten this system.	MedSite is not a priority for ABC Systems. This prolongs downtime for PIDS.
Natural Disasters	
Give examples of how *natural disasters* could threaten this system.	MedSite is located on a flood plane. We have had a history of floods, especially in the past five years. Access to PIDS was interrupted each time.

Areas of Concern

	Power Supply Problems
	Telecommunications Problems
	Third-Party Problems
ABC Systems' configuration of our firewall restricts access to important Internet medical sites. They do not understand our requirements.	
	Natural Disasters

Other Problems (cont.) **Basic Risk Profile**

Step 12

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Step 22

Impact Values

What is the potential impact on the organization in each applicable area?

Asset	Actor	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other
PIDS	physical configuration or arrangement of buildings, offices, or equipment	disclosure	H	H	L	M	L	-
		modification						
		loss, destruction						
		interruption						
		disclosure						
		modification						
		loss, destruction						
		interruption						
		disclosure						
		modification						
		loss, destruction						
		interruption						
		disclosure						
		modification						
		loss, destruction						
		interruption						

Basic Risk Profile

Other Problems (cont.)

Step 24

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value	Confidence	Very	Somewhat	Not At All
H	|X----|------|			
	|------|------|			
	|------|------|			
	|------|------|			
	|------|------|			
	|------|------|			
	|------|------|			
	|------|------|			
	|------|------|			
	|------|------|			
	|------|------|			
	|------|------|			
	|------|------|			
	|------|------|			
	|------|------|			
	|------|------|			

Step 26

Security Practice Areas

What is the stoplight status for each security practice area?

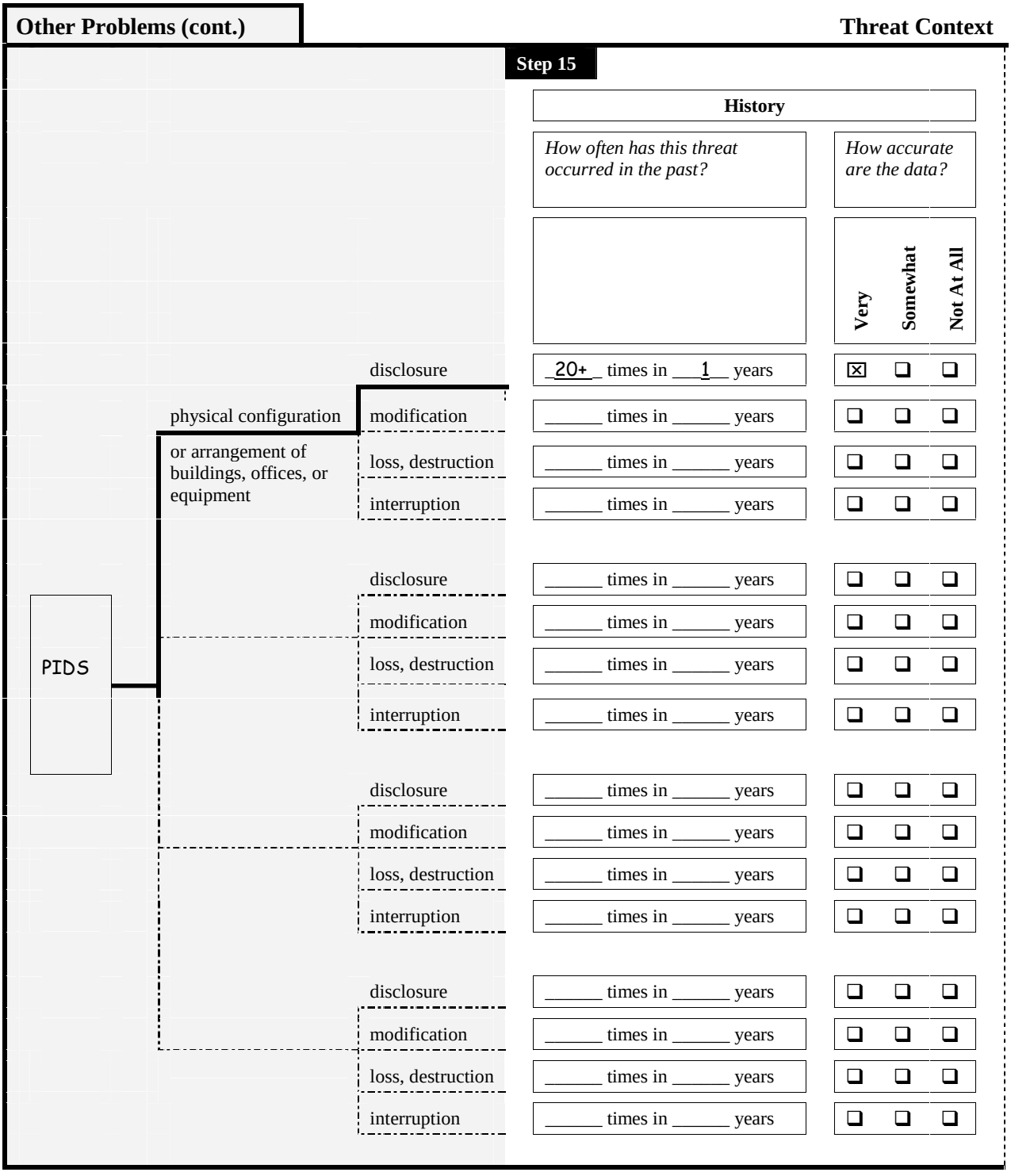
	Strategic						Operational								
	1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt
	R	R	R	Y	R	Y	Y	R							Y

Step 27

Approach

What is your approach for addressing each risk?

Accept	Defer	Mitigate
❑	☒	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑
❑	❑	❑


Other Problems (cont.)
Threat Context
Step 15
History
How often has this threat occurred in the past?
How accurate are the data?
Very
Somewhat
Not At All
PIDS
physical configuration or arrangement of buildings, offices, or equipment
disclosure
modification
loss, destruction
interruption
_20+_ times in ___1__ years
_____ times in _____ years

Threat Context | **Other Problems (cont.)**

Notes
What additional notes about each threat do you want to record?

Step 16

Other Problems (cont.)	**Areas of Concern**
Physical Configuration Problems	
Give examples of how *physical configuration of buildings, offices, or equipment* could threaten this system.	Physical configuration of work areas permits unauthorized viewing of private patient information by staff members as well as outsiders.
Give examples of how _____ could threaten this system.	
Give examples of how _____ could threaten this system.	
Give examples of how _____ could threaten this system.	

Areas of Concern

	Physical Configuration Problems

10 Risk Profile Worksheet for ABC Systems – Other Problems

Other Problems | **Basic Risk Profile**

Step 12 | **Step 22**

Threat

For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.

For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.

Impact Values

What is the potential impact on the organization in each applicable area?

Asset	Actor	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other
ABC Systems	key people taking a temporary leave of absence (e.g., due to illness, disability)	disclosure						
		modification						
		loss, destruction						
		interruption						
	key people leaving the organization permanently (e.g., retirement, other opportunities)	disclosure						
		modification						
		loss, destruction						
		interruption						
	threats affecting ~~a third-party or service provider~~ ABC Systems	disclosure						
		modification						
		loss, destruction						
		interruption	L	L	L	L	L	-
		disclosure						
		modification						
		loss, destruction						
		interruption						

Basic Risk Profile | **Other Problems**

Step 24 | **Step 26** | **Step 27**

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Security Practice Areas

What is the stoplight status for each security practice area?

Approach

What is your approach for addressing each risk?

Value	Confidence	Strategic						Operational									Approach		
	Very Somewhat Not At All	1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt	Accept	Defer	Mitigate
	|--------|--------|															❑	❑	❑
	|--------|--------|															❑	❑	❑
	|--------|--------|															❑	❑	❑
	|--------|--------|															❑	❑	❑
	|--------|--------|															❑	❑	❑
	|--------|--------|															❑	❑	❑
	|--------|--------|															❑	❑	❑
	|--------|--------|															❑	❑	❑
	|--------|--------|															❑	❑	❑
	|--------|--------|															❑	❑	❑
	|--------|--------|															❑	❑	❑
L	|--------|------X|	R		R		R	Y									☒	❑	❑
	|--------|--------|															❑	❑	❑
	|--------|--------|															❑	❑	❑
	|--------|--------|															❑	❑	❑
	|--------|--------|															❑	❑	❑

Other Problems

Threat Context

Step 15

			History			
			How often has this threat occurred in the past?	*How accurate are the data?*		
				Very	**Somewhat**	**Not At All**
ABC Systems	key people taking a temporary leave of absence (e.g., due to illness, disability)	disclosure	_____ times in _____ years	❑	❑	❑
		modification	_____ times in _____ years	❑	❑	❑
		loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑
	key people leaving the organization permanently (e.g., retirement, other opportunities)	disclosure	_____ times in _____ years	❑	❑	❑
		modification	_____ times in _____ years	❑	❑	❑
		loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑
	threats affecting ~~a third-party or service provider~~ ABC Systems	disclosure	_____ times in _____ years	❑	❑	❑
		modification	_____ times in _____ years	❑	❑	❑
		loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	__1__ times in __5__ years	❑	❑	☒
		disclosure	_____ times in _____ years	❑	❑	❑
		modification	_____ times in _____ years	❑	❑	❑
		loss, destruction	_____ times in _____ years	❑	❑	❑
		interruption	_____ times in _____ years	❑	❑	❑

Threat Context	Other Problems

Notes
What additional notes about each threat do you want to record?
To our knowledge, there has been one time that security issues affected ABC Systems' service in the last 5 years.

Step 16

Other Problems	Areas of Concern
People Taking a Temporary Leave of Absence	
Give examples of how *key people taking a temporary leave of absence* could affect the ability of this person or group of people to provide critical services, skills, and knowledge.	
People Leaving the Organization Permanently	
Give examples of how *key people leaving the organization permanently* could affect the ability of this person or group of people to provide critical services, skills, and knowledge.	
Threats Affecting a Third-Party	
Give examples of how *threats affecting a third party or service provider* could affect the ability of that third party or service provider to provide critical services, skills, and knowledge.	ABC Systems configures and maintains all major systems and the network for MedSite. If ABC Systems is unable to provide services to MedSite because of threats to their systems and networks, MedSite's operations could be affected.

Areas of Concern

People Taking a Temporary Leave of Absence
People Leaving the Organization Permanently
Threats Affecting a Third-Party
If there is a problem with PIDS or the network and ABC Systems is unable to respond in a timely manner, MedSite's downtime could be increased.

11 Network Access Paths Worksheet

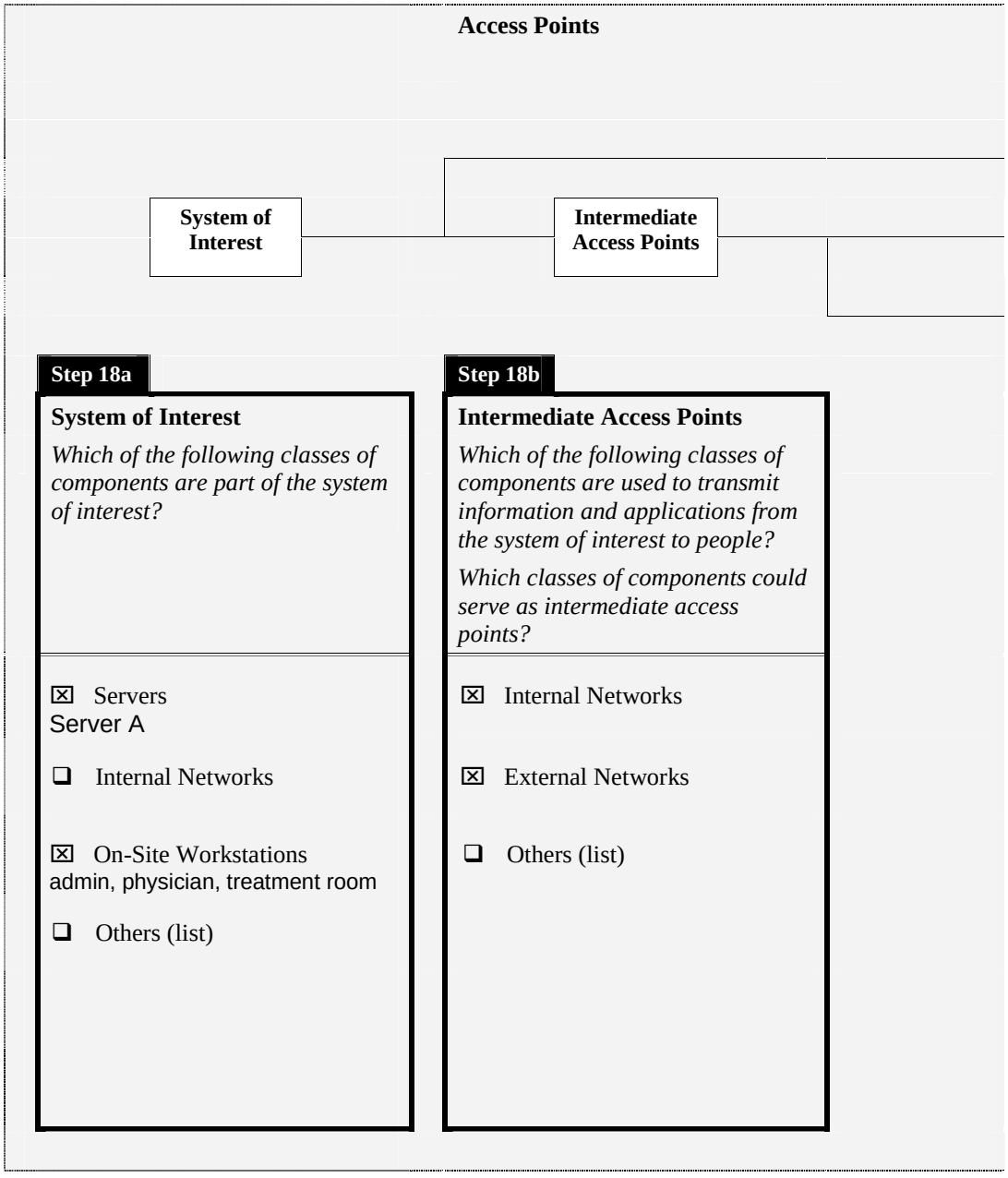
Steps 17 and 18

Step 17

System of Interest

What system or systems are most closely related to the critical asset?

PIDS (is its own system of interest)



Step 18a

System of Interest

Which of the following classes of components are part of the system of interest?

☒ Servers
Server A

❑ Internal Networks

☒ On-Site Workstations
admin, physician, treatment room

❑ Others (list)

Step 18b

Intermediate Access Points

Which of the following classes of components are used to transmit information and applications from the system of interest to people?

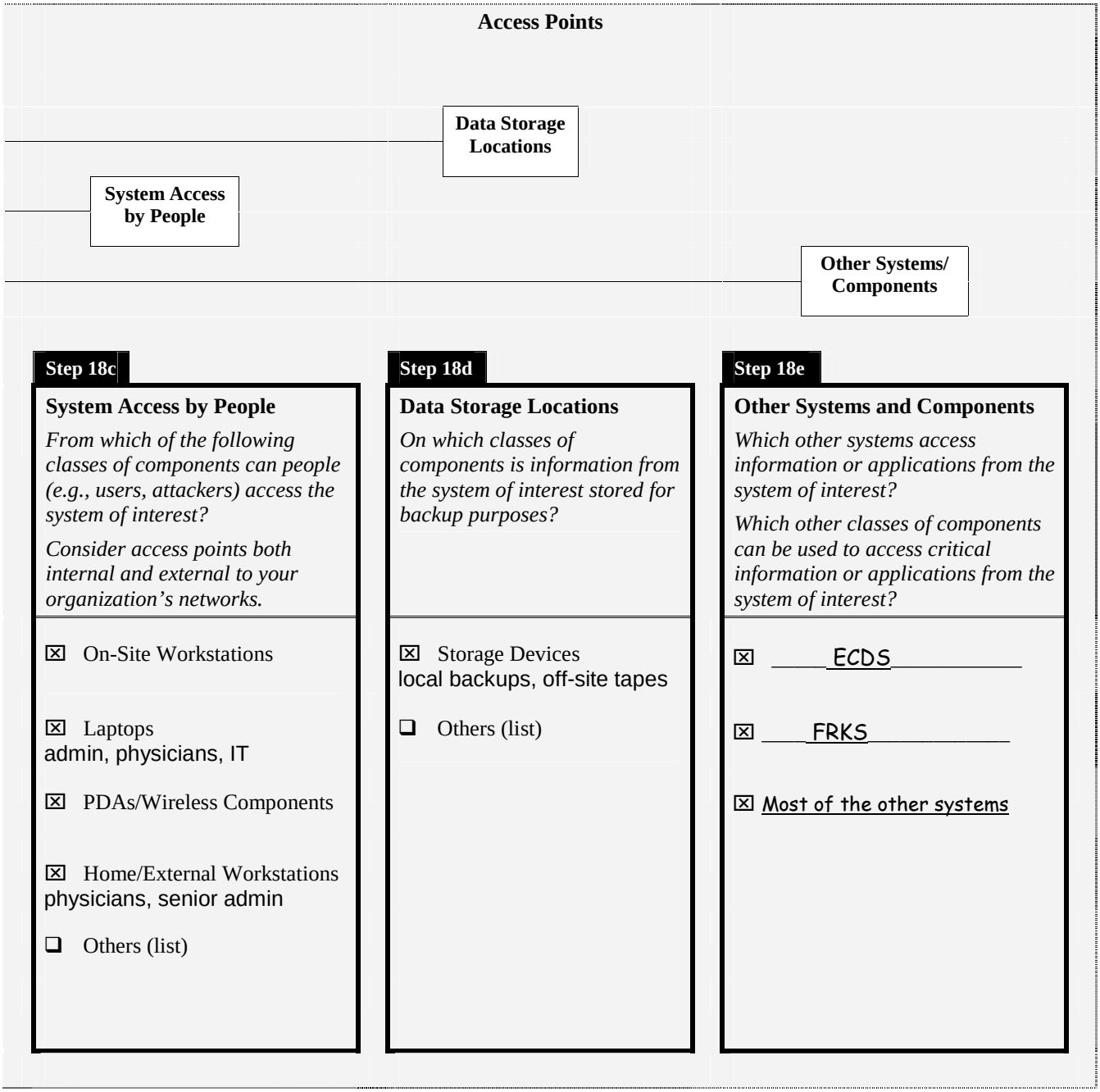
Which classes of components could serve as intermediate access points?

☒ Internal Networks

☒ External Networks

❑ Others (list)

Note: When you select a key class of components, make sure that you also document any relevant subclasses or specific examples when appropriate.



Step 18c

System Access by People

From which of the following classes of components can people (e.g., users, attackers) access the system of interest?

Consider access points both internal and external to your organization's networks.

- ☒ On-Site Workstations
- ☒ Laptops
  admin, physicians, IT
- ☒ PDAs/Wireless Components
- ☒ Home/External Workstations
  physicians, senior admin
- ❑ Others (list)

Step 18d

Data Storage Locations

On which classes of components is information from the system of interest stored for backup purposes?

- ☒ Storage Devices
  local backups, off-site tapes
- ❑ Others (list)

Step 18e

Other Systems and Components

Which other systems access information or applications from the system of interest?

Which other classes of components can be used to access critical information or applications from the system of interest?

- ☒ ECDS
- ☒ FRKS
- ☒ Most of the other systems

12 Infrastructure Review Worksheets

Steps 19, 20, and 21

Note
In Step 19a, mark the path to each class selected in Steps 18a-18e.

Step 19a	Step 19b					Step 20
Class *Which classes of components are related to one or more critical assets?* *(Document any relevant subclasses or specific examples when appropriate.)*	**Critical Assets** *Which critical assets are related to each class?* 1. PIDS	2. paper med recs	3. PCs	4. ABC Systems	5. ECDS	**Responsibility** *Who is responsible for maintaining and securing each class of component?*
Servers						
Server A	✓		✓			ABC Systems
Server B			✓		✓	ABC Systems
Internal Networks						
All	✓		✓		✓	ABC Systems & our IT
On-Site Workstations						
Admin	✓		✓		✓	ABC Systems & our IT
Physicians	✓		✓		✓	ABC Systems & our IT
Patient treatment rooms	✓		✓		✓	ABC Systems & our IT
Laptops						
Admin	✓		✓		✓	ABC Systems & our IT
Physicians	✓		✓		✓	ABC Systems & our IT
IT	✓		✓		✓	ABC Systems & our IT
PDAs/Wireless Components						
Physicians	✓					ABC Systems & our IT
Others	✓					ABC Systems & our IT
						ABC Systems & our IT

Step 21

Protection							**Notes/Issues**
To what extent is security considered when configuring and maintaining each class of component?				*How do you know?*			*What additional information do you want to record?*
Very Much	**Somewhat**	**Not At All**	**Don't Know**	**Formal Techniques**	**Informal Means**	**Other**	
Servers							
|----------|----------|			☒	❑	❑	❑	
|----------|----------|			☒	❑	❑	❑	
|----------|----------|			❑	❑	❑	❑	
Internal Networks							
|----------|------X-------|			❑	❑	☒	❑	IT does some items on these.
|----------|----------|			❑	❑	❑	❑	
|----------|----------|			❑	❑	❑	❑	
On-Site Workstations							
|---------X-|----------|			❑	❑	☒	❑	IT focuses on Admin's workstations.
|----------|--X----------|			❑	❑	☒	❑	
|----------|--X----------|			❑	❑	☒	❑	
Laptops							
|----------|----------|			☒	❑	❑	❑	
|----------|--X----------|			❑	❑	☒	❑	
|--X---------|----------|			❑	❑	☒	❑	IT does a lot of extras on their own PCs.
PDAs/Wireless Components							
|----------|----------X|			❑	❑	☒	❑	No one has paid attention to this.
|----------|----------X|			❑	❑	☒	❑	
|----------|----------|			❑	❑	❑	❑	

Note
In Step 19a, mark the path to each class selected in Steps 18a-18e.

Step 19a	Step 19b					Step 20
Class *Which classes of components are related to one or more critical assets?* *(Document any relevant subclasses or specific examples when appropriate.)*	**Critical Assets** *Which critical assets are related to each class?*					**Responsibility** *Who is responsible for maintaining and securing each class of component?*
	1. PIDS	2. paper med recs	3. PCs	4. ABC Systems	5. ECDS	
Other Systems						
All other systems	✓		✓		✓	ABC Systems and our IT
Storage Devices						
Local back-up	✓		✓		✓	ABC Systems and our IT
Off-site tapes	✓				✓	Not sure
External Networks						
All	✓					Unknown
Home/External Workstations						
Physicians, senior admin.	✓					Individual
Other _____						

Step 21

Protection							**Notes/Issues**
To what extent is security considered when configuring and maintaining each class of component?				*How do you know?*			*What additional information do you want to record?*
Very Much	**Somewhat**	**Not At All**	**Don't Know**	**Formal Techniques**	**Informal Means**	**Other**	
Other Systems							
|----------|---------X----|			❑	❑	☒	❑	
|----------|----------|			❑	❑	❑	❑	
|----------|----------|			❑	❑	❑	❑	
Storage Devices							
|----------|----------|			☒	❑	❑	❑	
|----------|----------|			☒	❑	❑	❑	Might be outsourced from ABC Systems
|----------|----------|			❑	❑	❑	❑	
External Networks							
|----------|----------|			☒	❑	❑	❑	
|----------|----------|			❑	❑	❑	❑	
|----------|----------|			❑	❑	❑	❑	
Home/External Workstations							
|----------|----------|			☒	❑	❑	❑	Up to owner to manage
|----------|----------|			❑	❑	❑	❑	
|----------|----------|			❑	❑	❑	❑	
Other _____							
|----------|----------|			❑	❑	❑	❑	
|----------|----------|			❑	❑	❑	❑	
|----------|----------|			❑	❑	❑	❑	

13 Probability Evaluation Criteria Worksheet

Step 23

Step 23

Frequency-Based Criteria

1. *Think about what constitutes a high, medium, and low likelihood of occurrence for threats to your organization's critical assets.*

	High				Medium
Time Between Events	Daily	Weekly	Monthly	Four Times Per Year	< 4 Times Per Year ~~Two Times Per Year~~
Annualized Frequency	365	52	12	4	~~2~~ < 4

2. *Draw lines that separate high from medium and medium from low.*

Medium	Low				
One Time Per Year	< 1 Time Per Year ~~Once Every Two Years~~	Once Every Five Years	Once Every 10 Years	Once Every 20 Years	Once Every 50 Years
1	~~0.5~~ < 1	0.2	0.1	0.05	0.02

14 Protection Strategy Worksheet

Steps 25, 29

This section includes an excerpt of the entire protection strategy for MedSite. Two types of practice areas are included: the selected mitigation areas and a few of the other practice areas with general, strategic improvements.

The mitigation areas reflect corporate or strategic-level changes driven primarily by the mitigation plans for specific risks to critical assets. The mitigation areas are

- Security awareness and training
- Collaborative security management
- Monitoring and auditing physical security
- Authentication and authorization

Strategic level changes were also identified for the rest of the security practice areas. The other areas with strategic changes included here are security policies and regulations.

14.1 Protection Strategy for Security Awareness and Training

1. Security Awareness and Training

Stoplight Status R

Step 25: How formal is your organization's training strategy?

Step 29: Will any mitigation activities change your training strategy?
Do you want to make any additional changes to your training strategy?

Training Strategy	Step 25	Step 29
The organization has a documented training strategy that includes security awareness training and security-related training for supported technologies.	❑ Current	❑ Change
The organization has an informal and undocumented training strategy.	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: How often is security awareness training provided?

Step 29: Will any mitigation activities change how often security awareness training is provided?
Do you want to make any additional changes to how often security awareness training is provided?

Security Awareness Training	Step 25	Step 29
Periodic security awareness training is provided for all employees ____1____time(s) every ____1____ years.	❑ Current	☒ Change
Security awareness training is provided for new staff members as part of their orientation activities.	☒ Current	❑ Change
The organization does not provide security awareness training. Staff members learn about security issues on their own.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

1. Security Awareness and Training

Step 25: To what extent are IT staff members required to attend security-related training?

Step 29: Will any mitigation activities change the requirement for attending security-related training?
Do you want to make any additional changes to the requirement for attending security-related training?

Security-Related Training for Supported Technologies	Step 25	Step 29
Information technology staff members are required to attend security-related training for any technologies that they support.	❑ Current	❑ Change
Information technology staff members can attend security-related training for any technologies that they support if they request it.	❑ Current	☒ Change
The organization generally does not provide opportunities for information technology staff members to attend security-related training for supported technologies. Information technology staff members learn about security-related issues on their own.	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: How formal is your organization's mechanism for providing periodic security updates?

Step 29: Will any mitigation activities change your mechanism for providing periodic security updates?
Do you want to make any additional changes to your mechanism for providing periodic security updates?

Periodic Security Updates	Step 25	Step 29
The organization has a formal mechanism (including coordination with ABC Systems) for providing staff members with periodic updates/bulletins about important security issues.	❑ Current	☒ Change
The organization does not have a mechanism for providing staff members with periodic updates/bulletins about important security issues.	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

1. Security Awareness and Training

Stoplight Status R

Step 25: How formal is your organization's mechanism for verifying that staff receives training?

Step 29: Will any mitigation activities change your mechanism for verifying that staff receives training?
Do you want to make any additional changes to your mechanism for verifying that staff receives training?

Training Verification	Step 25	Step 29
The organization has formal mechanisms for tracking and verifying that staff members receive appropriate security-related training.	❑ Current	❑ Change
The organization has informal mechanisms for tracking and verifying that staff members receive appropriate security-related training.	❑ Current	☒ Change
The organization has no mechanisms for tracking and verifying that staff members receive appropriate security-related training.	☒ Current	❑ Change
_____	❑ Current	❑ Change

Step 25: What additional characteristic of your current approach to security awareness and training do you want to record?

Step 29: Will any mitigation activities change this characteristic?
Do you want to make any additional changes to this characteristic?

Other:	Step 25	Step 29
_____	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____	❑ Current	❑ Change

14.2 Protection Strategy for Collaborative Security Management

5. Collaborative Security Management

Stoplight Status R

*Step 25: How formal are your organization's policies and procedures for protecting information when working with **collaborators and partners**?*

Step 29: Will any mitigation activities change the policies and procedures for protecting information when working with collaborators and partners?
Do you want to make any additional changes to the policies and procedures for protecting information when working with collaborators and partners?

Collaborators and Partners	Step 25	Step 29
The organization has documented policies and procedures for protecting information when working with collaborators and partners.	❑ Current	❑ Change
The organization has documented policies and procedures for protecting certain information when working with collaborators and partners. The organization has informal and undocumented policies and procedures for protecting other types of information when working with collaborators and partners.	❑ Current	❑ Change
The organization has informal and undocumented policies and procedures for protecting information when working with collaborators and partners.	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

*Step 25: How formal are your organization's policies and procedures for protecting information when working with **contractors and subcontractors**?*

Step 29: Will any mitigation activities change the policies and procedures for protecting information when working with contractors and subcontractors?
Do you want to make any additional changes to the policies and procedures for protecting information when working with contractors and subcontractors?

Contractors and Subcontractors	Step 25	Step 29
The organization has documented policies and procedures for protecting information when working with contractors and subcontractors.	❑ Current	❑ Change
The organization has documented policies and procedures for protecting certain information when working with contractors and subcontractors. The organization has informal and undocumented policies and procedures for protecting other types of information when working with contractors and subcontractors.	❑ Current	❑ Change
The organization has informal and undocumented policies and procedures for protecting information when working with contractors and subcontractors.	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

5. Collaborative Security Management

*Step 25: How formal are your organization's policies and procedures for protecting information when working with **service providers**?*

Step 29: Will any mitigation activities change the policies and procedures for protecting information when working with service providers?
Do you want to make any additional changes to the policies and procedures for protecting information when working with service providers?

Service Providers	Step 25	Step 29
The organization has documented policies and procedures for protecting information when working with service providers.	❑ Current	❑ Change
The organization has documented policies and procedures for protecting certain information when working with service providers. The organization has informal and undocumented policies and procedures for protecting other types of information when working with service providers.	❑ Current	❑ Change
The organization has informal and undocumented policies and procedures for protecting information when working with service providers.	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization formally communicate its information protection requirements to third parties?

Step 29: Will any mitigation activities change how your organization communicates its information protection requirements to third parties?
Do you want to make any additional changes to how your organization communicates its information protection requirements to third parties?

Requirements	Step 25	Step 29
The organization documents information protection requirements and explicitly communicates them to all appropriate third parties.	❑ Current	❑ Change
The organization informally communicates information protection requirements to ~~all appropriate third parties~~. Facilities Management and ABC Systems.	❑ Current	☒ Change
The organization does not communicate information protection requirements to third parties.	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

5. Collaborative Security Management

Stoplight Status R

Step 25: To what extent does your organization verify that third parties are addressing information protection requirements?

Step 29: Will any mitigation activities change verification mechanisms?
Do you want to make any additional changes to verification mechanisms?

Verification	Step 25	Step 29
The organization has formal mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.	❑ Current	❑ Change
Facilities Management and ABC Systems The organization has informal mechanisms for verifying that ~~all third-party organizations, outsourced security services, mechanisms, and technologies~~ meet its needs and requirements.	❑ Current	☒ Change
The organization has no mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your security-awareness training program include information about collaborative security management?

Step 29: Will any mitigation activities change the content of your security awareness training to include information about collaborative security management?
Do you want to make any additional changes to the content of your security awareness training?

Staff Awareness	Step 25	Step 29
The organization's security-awareness training program includes information about the organization's collaborative security management policies and procedures. This training is provided for all employees _____time(s) every _____ years.	❑ Current	❑ Change
The organization's security-awareness training program includes information about the organization's collaborative security management policies and procedures. This training is provided for new staff members as part of their orientation activities.	❑ Current	❑ Change
The organization's security-awareness training program does not include information about the organization's collaborative security management policies and procedures. Staff members learn about collaborative security management policies and procedures on their own.	☒ Current	❑ Change
_____	❑ Current	❑ Change

5. Collaborative Security Management

Step 25: What additional characteristic of your current approach to collaborative security management do you want to record?

Step 29: Will any mitigation activities change this characteristic?
Do you want to make any additional changes to this characteristic?

Other:	**Step 25**	**Step 29**
_____ _____	❑ Current	❑ Change
_____ _____	❑ Current	❑ Change
_____ _____	❑ Current	❑ Change

14.3 Protection Strategy for Monitoring and Auditing Physical Security

8. Monitoring and Auditing Physical Security

Stoplight Status R

Step 25: Who is currently responsible for monitoring and auditing physical security?

Step 29: Will any mitigation activities change responsibility for monitoring and auditing physical security? Do you want to make any additional changes affecting responsibility for monitoring and auditing physical security?

Responsibility	**Step 25**			**Step 29**		
	☒ Current			❑ Change		
Task	Internal	External	Combined	Internal	External	Combined
Keeping maintenance records to document repairs and modifications to IT hardware	❑	❑	☒	❑	❑	❑
Monitoring physical access to controlled IT hardware	❑	❑	☒	❑	❑	❑
Monitoring physical access to controlled IT software media	❑	❑	☒	❑	❑	❑
Monitoring physical access to restricted work areas	❑	❑	☒	❑	❑	❑
Reviewing monitoring records on a periodic basis	❑	❑	☒	❑	❑	❑
Investigating and addressing any unusual activity that is identified	❑	❑	☒	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑

8. Monitoring and Auditing Physical Security

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area? Do you want to make any additional changes to how procedures are documented for this area?

Procedures	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented plans and procedures for monitoring physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization has some formally documented policies and procedures for monitoring physical access to ~~the building and premises, work areas~~, IT hardware, and software media. Some policies and procedures in this area are informal and undocumented.	❑ Current	☒ Change
The organization has informal and undocumented plans and procedures for monitoring physical access to ~~the building and premises, work areas~~, IT hardware, and software media.	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area? Do you want to make any additional changes to the requirement for attending training in this area?

Training	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
Designated staff members are required to attend training for monitoring physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
Designated staff members can attend training for monitoring physical access to the building and premises, work areas, IT hardware, and software media if they request it.	❑ Current	❑ Change
The organization generally does not provide opportunities for designated staff members to attend training for monitoring physical access to ~~the building and premises, work areas~~, IT hardware, and software media. Designated staff members learn about monitoring physical access on their own.	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

8. Monitoring and Auditing Physical Security

Stoplight Status R

Third Party A: Facilities Management

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for monitoring physical security are formally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization's requirements for monitoring physical security are informally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, ~~IT hardware, and software media~~.	❑ Current	☒ Change
The organization's requirements for monitoring physical security are not communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, ~~IT hardware, and software media.~~	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for monitoring physical security.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for monitoring physical security.	❑ Current	☒ Change
The organization does not verify that contractors and service providers have met the requirements for monitoring physical security.	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

8. Monitoring and Auditing Physical Security

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for monitoring physical security are formally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization's requirements for monitoring physical security are informally communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
The organization's requirements for monitoring physical security are not communicated to all contractors and service providers that monitor physical access to the building and premises, work areas, IT hardware, and software media.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to how you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for monitoring physical security.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for monitoring physical security.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for monitoring physical security.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

14.4 Protection Strategy for Authentication and Authorization

11. Authentication and Authorization

Stoplight Status R

Step 25: Who is currently responsible for authentication and authorization?

Step 29: Will any mitigation activities change responsibility for authentication and authorization?
Do you want to make any additional changes affecting responsibility for authentication and authorization?

Responsibility	**Step 25**			**Step 29**		
	☒ Current			☒ Change		
Task	Internal	External	Combined	Internal	External	Combined
Implementing access controls (e.g., file permissions, network configuration) to restrict user access to information, sensitive systems, specific applications and services, and network connections	❑	☒	❑	❑	❑	☒
Implementing user authentication (e.g., passwords, biometrics) to restrict user access to information, sensitive systems, specific applications and services, and network connections	❑	☒	❑	❑	❑	☒
Establishing and terminating access to systems and information for both individuals and groups	❑	❑	☒	❑	❑	☒
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑
_____	❑	❑	❑	❑	❑	❑

11. Authentication and Authorization

Step 25: To what extent are procedures for this area formally documented?

Step 29: Will any mitigation activities change the extent to which procedures are formally documented for this area? Do you want to make any additional changes to how procedures are documented for this area?

Procedures	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
The organization has formally documented authorization and authentication procedures for restricting user access to information, sensitive systems, specific applications and services, and network connections.	❑ Current	❑ Change
The organization has some formally documented authorization and authentication procedures for restricting user access to information, sensitive systems, specific applications and services, and network connections. Some procedures in this area are informal and undocumented.	❑ Current	☒ Change
The organization has informal and undocumented authorization and authentication procedures for restricting user access to information, sensitive systems, specific applications and services, and network connections.	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent are staff members required to attend training in this area?

Step 29: Will any mitigation activities change the requirement for attending training in this area? Do you want to make any additional changes to the requirement for attending training in this area?

Training	**Step 25**	**Step 29**
If staff from your organization is partly or completely responsible for this area:		
Information technology staff members are required to attend training for implementing technological measures to restrict user access to information, sensitive systems, specific applications and services, and network connections.	❑ Current	❑ Change
Information technology staff members can attend training for implementing technological measures to restrict user access to information, sensitive systems, specific applications and services, and network connections if they request it.	❑ Current	☒ Change
The organization generally does not provide opportunities for information technology staff members to attend training for implementing technological measures to restrict user access to information, sensitive systems, specific applications and services, and network connections. Information technology staff members learn about authentication and authorization on their own.	☒ Current	❑ Change
_____	❑ Current	❑ Change

11. Authentication and Authorization

Stoplight Status R

Third Party A: ABC Systems

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for controlling access to systems and information are formally communicated to all contractors and service providers that provide authentication and authorization services.	❑ Current	❑ Change
The organization's requirements for controlling access to systems and information are informally communicated to all contractors and service providers that monitor systems and networks.	❑ Current	☒ Change
The organization's requirements for controlling access to systems and information are not communicated to all contractors and service providers that monitor systems and networks.	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to you verify that requirements are being met?

Verification	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for authentication and authorization.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for authentication and authorization.	❑ Current	☒ Change
The organization does not verify that contractors and service providers have met the requirements for authentication and authorization.	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

11. Authentication and Authorization

Third Party B:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	**Step 25**	**Step 29**
If staff from a third party is partly or completely responsible for this area:		
The organization's requirements for controlling access to systems and information are formally communicated to all contractors and service providers that provide authentication and authorization services.	❑ Current	❑ Change
The organization's requirements for controlling access to systems and information are informally communicated to all contractors and service providers that monitor systems and networks.	❑ Current	❑ Change
The organization's requirements for controlling access to systems and information are not communicated to all contractors and service providers that monitor systems and networks.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your organization verify that this third party is addressing requirements in this area?

Step 29: Will any mitigation activities change how you verify that this third party is addressing requirements in this area? Do you want to make any additional changes to you verify that requirements are being met?

Verification	**Step 25**	**Step 29**
If staff from a third party is partly or completely responsible for this area:		
The organization formally verifies that contractors and service providers have met the requirements for authentication and authorization.	❑ Current	❑ Change
The organization informally verifies that contractors and service providers have met the requirements for authentication and authorization.	❑ Current	❑ Change
The organization does not verify that contractors and service providers have met the requirements for authentication and authorization.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

14.5 Protection Strategy for Security Policies and Regulations

4. Security Policies and Regulations

Stoplight Status | Y |

Step 25: To what extent are your organization's security-related policies formally documented?

Step 29: Will any mitigation activities change the extent to which your security-related policies are formally documented? Do you want to make any additional changes to the extent to which your security-related policies are formally documented?

Documented Policies	Step 25	Step 29
The organization has a comprehensive set of formally documented security-related policies.	❑ Current	❑ Change
The organization has a partial set of formally documented security-related policies. Some security-related policies are informal and undocumented.	☒ Current	❑ Change
The organization's security-related policies are informal and undocumented.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: How formal is your organization's mechanism for creating and updating its security-related policies?

Step 29: Will any mitigation activities change how your security-related policies are created and updated? Do you want to make any additional changes to how your security-related policies are created and updated?

Policy Management	Step 25	Step 29
The organization has a formal mechanism for creating and updating its security-related policies.	❑ Current	❑ Change
The organization has a formal mechanism for creating its security-related policies. The organization has an informal and undocumented mechanism for updating its security-related policies.	❑ Current	❑ Change
The organization has an informal and undocumented mechanism for creating and updating its security-related policies.	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

4. Security Policies and Regulations

Step 25: How formal are your organization's procedures for enforcing its security-related policies?

Step 29: Will any mitigation activities change how security-related policies are enforced?
Do you want to make any additional changes to how security-related policies are enforced?

Policy Enforcement	Step 25	Step 29
The organization has formal procedures for enforcing its security-related policies. Enforcement procedures are consistently followed.	❑ Current	❑ Change
The organization has formal procedures for enforcing its security-related policies. Enforcement procedures are inconsistently followed.	❑ Current	☒ Change
The organization has informal and undocumented procedures for enforcing its security-related policies.	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

Step 25: To what extent does your security-awareness training program include information about the organization's security policies and regulations?

Step 29: Will any mitigation activities change the content of your security awareness training to include security policy and regulation information?
Do you want to make any additional changes to the content of your security awareness training?

Staff Awareness	Step 25	Step 29
The organization's security-awareness training program includes information about the organization's security policies and regulations. This training is provided for all employees ____1____time(s) every ____1____ years.	❑ Current	☒ Change
The organization's security-awareness training program includes information about the organization's security policies and regulations. This training is provided for new staff members as part of their orientation activities.	❑ Current	❑ Change
The organization's security-awareness training program does not include information about the organization's security policies and regulations. Staff members learn about security policies and regulations on their own.	☒ Current	❑ Change
_____	❑ Current	❑ Change
_____		

4. Security Policies and Regulations

Stoplight Status | Y |

Step 25: How formal are your organization's procedures for complying with security-related policies and regulations?

Step 29: Will any mitigation activities change how your organization complies with security-related policies and regulations?
Do you want to make any additional changes to how your organization complies with security-related policies and regulations?

Policy and Regulation Compliance	Step 25	Step 29
The organization has formal procedures for complying with information security policies, applicable laws and regulations, and insurance requirements.	❑ Current	❑ Change
The organization has formal procedures for complying with certain information security policies, applicable laws and regulations, and insurance requirements. Some procedures in this area are informal and undocumented.	❑ Current	☒ Change
The organization has informal and undocumented procedures for complying with information security policies, applicable laws and regulations, and insurance requirements.	☒ Current	❑ Change
_____	❑ Current	❑ Change

Step 25: What additional characteristic of your current approach to security policies and regulations do you want to record?

Step 29: Will any mitigation activities change this characteristic?
Do you want to make any additional changes to this characteristic?

Other:	Step 25	Step 29
_____	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____	❑ Current	❑ Change

15 Mitigation Plan Worksheet

Step 28

Mitigation Area: 1. Security Awareness and Training

Step 28

Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*
Provide periodic security awareness training for all employees once a year. Note: This will change MedSite's protection strategy.	MedSite's current policy is to provide awareness training for new employees only. This is inadequate. Security awareness training should be provided on a periodic basis.
Enable IT staff members to attend security-related training for any technologies that they support.	The security practices survey indicated that there is a lack of training for IT staff at MedSite.
The manager in each department will keep a list of people who have received security awareness training and when they received it.	We must set up a tracking mechanism if we intend to improve our training related to security.

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*
MedSite's senior management team and the training department manager	Increasing the frequency of security awareness training requires commitment and funding from senior management. It will also require a commitment from MedSite's Training Department.
MedSite's IT manager must take responsibility for implementing this mitigation activity.	MedSite's senior managers must approve and find funding for this activity. MedSite's CIO needs to sponsor implementation of this activity.
The manager in each MedSite department	Each department manager must participate in this activity. Senior managers need to make this a requirement for it to work.

Mitigation Area: 5. Collaborative Security Management

Step 28

Mitigation Activity	**Rationale**
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*
Designate an IT staff member as point of contact to communicate our requirements for protecting PIDS information to ABC Systems. Designate staff member from the Maintenance Department to communicate our physical security requirements for building security to the Facilities Management Group. Note: This will change MedSite's protection strategy.	We are currently doing nothing with respect to communicating security requirements to ABC Systems and the Facilities Management Group. Establishing a point of contact for each organization should improve communication of our requirements.
The IT point of contact will verify that requirements for protecting PIDS information are met by ABC Systems. The Maintenance Department point of contact will verify that requirements for physical security are met by the Facilities Management Group for the building. Note: This will change MedSite's protection strategy.	If we are establishing a means to communicate our requirements to ABC Systems and the Facilities Management Group, then we need the points of contact to make sure that those requirements have been met.
Contract with ABC Systems to send security bulletins to MedSite's IT point of contact, who will forward the bulletins to MedSite's staff.	MedSite's staff is not receiving information about security problems, such as viruses.

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*
TBD – Responsibility must be assigned by MedSite's CIO and the manager of the Maintenance Department.	MedSite's senior management team must sponsor this activity. The CIO and manager of the Maintenance Department must assign the points of contact.
TBD – A point of contact must be assigned to work with ABC Systems. A point of contact must be assigned to work with the Facilities Management Group.	MedSite's senior management team must sponsor this activity. The CIO and manager of the Maintenance Department must assign the points of contact.
TBD – A point of contact must be assigned to work with ABC Systems.	MedSite's senior management team must sponsor this activity. The CIO must assign the point of contact.

Mitigation Area: 8. Monitoring and Auditing Physical Security

Step 28

Mitigation Activity	**Rationale**
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*
Document formal procedures for monitoring physical access to all IT hardware and software media. Note: This will change MedSite's protection strategy.	Some staff members from MedSite's IT department informally monitor the physical security of IT hardware and software. Formalizing the procedures would help to ensure that they are consistently applied by all IT staff members.
Assign a point of contact from MedSite to work with the Facilities Management Group to monitor physical access to the building and premises. The point of contact will be responsible for communicating MedSite's requirements for monitoring physical security and for verifying that the requirements have been met. Note: This will change MedSite's protection strategy.	Responsibility for monitoring and auditing physical security is assigned to the Facilities Management Group and MedSite. Activities are not coordinated among the two organizations. Establishing points of contact at MedSite to work with staff from the Facilities Management Group should improve communication of our requirements and improve how physical security is managed.

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*
TBD – A small team to document the procedures must be assigned by MedSite's CIO and/or IT manager.	MedSite's CIO must sponsor this activity and assign a small team to document the procedures.
TBD – A point of contact must be assigned to work with Facilities Management Group.	MedSite's senior management team must sponsor this activity. The manager of the Maintenance Department must assign the points of contact.

Mitigation Area: 11. Authentication and Authorization

Step 28

Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*
Assign joint responsibility for the following to MedSite and ABC Systems. – implementing access controls for PIDS – implementing user authentication for PIDS Note: This will change MedSite's protection strategy.	People from MedSite's IT department must participate in controlling access to PIDS. Staff at ABC Systems do not know who should have legitimate access to what.
Document procedures for controlling access to PIDS. Note: This will change MedSite's protection strategy.	Restricting user access is currently done in an ad hoc manner. MedSite's IT department must develop formalized procedures for restricting user access to ensure that they are consistently applied by all IT staff members. Procedures for implementing access controls must specify how to work with staff from ABC Systems.
Assign a point of contact from MedSite to work with ABC Systems to control access to PIDS. The point of contact will be responsible for communicating MedSite's requirements for controlling access to PIDS and for verifying that the requirements have been met. Note: This will change MedSite's protection strategy.	We are currently doing nothing with respect to communicating requirements to ABC Systems for controlling access to information and systems. Establishing a point of contact from MedSite's IT department should improve communication of our requirements.

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*
TBD – A point of contact must be assigned to work with ABC Systems.	MedSite's senior management team must sponsor this activity. The CIO must assign staff to work with ABC Systems.
TBD – A small team to document the procedures must be assigned by MedSite's CIO and/or IT manager. The team should include representation from the IT department and the point of contact for ABC Systems.	MedSite's senior management team must sponsor this activity. MedSite's CIO must sponsor this activity and assign a small team to document the procedures.
TBD – A point of contact must be assigned to work with ABC Systems.	MedSite's senior management team must sponsor this activity. The CIO must assign the point of contact.

Mitigation Area: __11. Authentication and Authorization_(cont.)_____

Step 28

Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*
Check all PIDS workstations in treatment rooms to ensure that access to those workstations automatically times out after a designated period of time.	Too many people, both staff and patients, have physical access to PIDS from workstations in treatment rooms. Unauthorized people could use this access to view a patient's medical records deliberately. Or a patient could accidentally see another patient's medical records. Privacy regulations makes this an important issue.

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*
TBD – MedSite's CIO and/or IT manager will identify the IT staff who will implement this activity. Designated staff will have to work with staff from ABC Systems to set automatic timeouts.	MedSite's senior management team must sponsor this activity. MedSite's CIO must sponsor this activity and assign a staff to set automatic timeouts.

Mitigation Area: 4. Security Policies and Regulations

Step 28

Mitigation Activity	Rationale
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*
Create procedures for complying with HIPAA data security regulations. Note: This will change MedSite's protection strategy.	MedSite has two years in which to be in compliance with the HIPAA data security requirements. Note: This activity is driven by the regulations rather than any specific risk.
Include information about MedSite's security-related policies and procedures in the new security awareness training. Note: This will change MedSite's protection strategy.	Few staff members are aware of or understand MedSite's security-related policies. This information must be featured in awareness training. Note: This activity is driven by general concerns rather than any specific risk.
Procedures for enforcing MedSite's security-related policies must be created. Note: This will change MedSite's protection strategy.	People's behaviors related to security will only change if they understand that management strictly enforces MedSite's security policies. Note: This activity is driven by general concerns rather than any specific risk.

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*
TBD – Responsibility must be assigned by MedSite's senior management team.	MedSite's senior management team must sponsor this activity.
MedSite's senior management team and the Training Department manager	Updating the content of security awareness training requires commitment and funding from senior management. It will also require a commitment from MedSite's Training Department.
MedSite's senior management team	MedSite's senior management team must sponsor this activity.

16 Next Steps Worksheet

Step 30

Step 30

Management Sponsorship for Security Improvement

What must management do to support the implementation of OCTAVE-S results?

Consider:

- Contribute funds to information security activities.
- Assign staff to information security activities.
- Ensure that staff members have sufficient time allocated to information security activities.
- Enable staff to receive training about information security.
- Make information security a strategic priority.

MTF management must

- allocate funds to implement the mitigation plans
- make information security a strategic priority

All functional managers must ensure that staff members have sufficient time to participate in any security-related activities to which they are assigned.

Monitoring Implementation
What will the organization do to track progress and ensure that the results of this evaluation are implemented?
Each team assigned responsibility for a risk mitigation plan will be responsible for scheduling and implementing that plan. Each team will provide a written status report prior to the monthly management team meeting.

Expanding the Current Information Security Risk Evaluation
Will you expand the current OCTAVE-S evaluation to include additional critical assets? Which ones?
No, but we will review all deferred risks within the next 30 days to see if anything else needs to be done for them. We will also do a gap analysis between the results of OCTAVE-S and current regulations (including HIPAA) and see if there are any other required practices that we should consider during another round of resource allocations in the next quarter.

Next Information Security Risk Evaluation
When will the organization conduct its next OCTAVE-S evaluation?
The next OCTAVE-S evaluation will be performed 12-15 months from now.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
OCTAVE-S Implementation Guide, Version 1.0, Volume 10	F19628-00-C-0003

6. AUTHOR(S)

Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody

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

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

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

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

14. SUBJECT TERMS	15. NUMBER OF PAGES
information security, risk management, OCTAVE	198

16. PRICE CODE

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