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



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

Unlimited distribution subject to the copyright.

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.

Copyright 2005 by Carnegie Mellon University.

® OCTAVE is registered in the U.S. Patent & Trademark Office by Carnegie Mellon University.

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

NO WARRANTY

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

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

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

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

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

OCTAVE-S V1.0 Table of Contents

Table of Contents

ADC	out This Documentv
Abs	stractvii
1	Introduction1
2	Critical Asset Information Worksheet for Systems5
3	Risk Profile Worksheet for Systems - Human Actors Using Network Access9
4	Risk Profile Worksheet for Systems - Human Actors Using Physical Access19
5	Risk Profile Worksheet for Systems - System Problems29
6	Risk Profile Worksheet for Systems - Other Problems39
7	Network Access Paths Worksheet55
8	Threat Translation Guide59

Table of Contents OCTAVE-S V1.0

OCTAVE-S V1.0 List of Tables

List of Tables

Γable 1:	Worksheets Provided in This Workbook	1
----------	--------------------------------------	---

List of Tables OCTAVE-S V1.0

OCTAVE-S V1.0 About This Document

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.

About This Document OCTAVE-S V1.0

OCTAVE-S V1.0 Abstract

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.

OCTAVE-S V1.0 Abstract

viii

OCTAVE-S V1.0 Introduction

1 Introduction

This document contains the Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (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 <i>Critical Asset Information worksheet</i> .	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 <i>Critical Asset Selection worksheet</i> . 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	

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.

Introduction OCTAVE-S V1.0

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 <i>Critical Asset Information worksheet</i> .	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 <i>Critical Asset Information worksheet</i> .	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 <i>Threat Translation Guide</i> .	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 <i>Risk Profile worksheet</i> 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

OCTAVE-S V1.0 Introduction

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

Step Description		scription Worksheet		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

Introduction OCTAVE-S V1.0

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

Step	Description	Worksheet	Activity	Pages	
Step 22	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.		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	9-54		
Step 26	Transfer the stoplight status for each security practice area from the <i>Security Practices worksheet</i> to the "Security Practice Areas" section (Step 26) of each critical asset's <i>Risk Profile worksheet</i> .	Risk Profile Security Practices	Phase 3 Process S5 S5.2 Select Mitigation Approaches	9-54	
Step 27	, and the second		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

	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 <i>Critical Asset Information worksheet</i> .
Step 8	Record a description for each critical asset on that asset's <i>Critical Asset Selection worksheet</i> . 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 <i>Critical Asset Information</i> worksheet. Refer to the <i>Asset Identification worksheet</i> to determine which assets are related
	to each critical asset. Phase 1
C4 10	Process S2 Activity S2.2
Step 10	Record the security requirements for each critical asset on that asset's <i>Critical Asset Information worksheet</i> .

For each critical asset, record the most important security requirement on that asset's

Critical Asset Information worksheet.

Step 11

OCTAVE-S V1.0

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	s system?
Then assets are related to this	, system.
nformation:	Applications:
Other:	

Who is responsible for the system?

Ste	p 10	Step 11		
Sec	urity Requiremen	Most Important Security Requirement		
:	at are the security nt: Focus on what	Which security requirement is most important for this system?		
<u> </u>	Confidentiality	Only authorized personnel can view information on		Confidentiality
				Integrity
۵	Integrity	Only authorized personnel can modify information on		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 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 Act	tors Using I	Network A	Access					Basic	Risk	Profile
Step 12					Step 2	22				
		Thr	eat				Impact	Values	;	
	branches is th Mark these bro		egligible possibil e tree.	ity of a threat to			otential in each			ea?
			is there a neglig Do not mark the	rible possibility or ese branches.						
Asset	Access	Actor	Motive	Outcome						
					Reputation	Financial	Productivity	Fines	Safety	Other
				disclosure						
			accidental	modification						
				loss, destruction						
		inside	_	interruption						
				disclosure						
			deliberate	modification						
	network			loss, destruction						
				interruption						
				disclosure						
			accidental	modification						
			-	loss, destruction						
		outside		interruption						
				disclosure						
			deliberate	modification						
				loss, destruction						
				interruption						

Basic Risk Profile		Human Actors Using N	letwork 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?	Secur. What is the stoplight status for ea	ity Practice Areas ach security practice area?	Approach What is your approach for addressing each risk?
Value Confidence	Strategic	Operational	
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

an Actors Using	TACLWOLK	Access		Threat Cor
				Threat Actors
				Which actors pose the biggest threats to this system via the network?
			disclosure	Insiders acting accidentally:
		accidental	modification	
			loss, destruction	
	inside	<u> </u> 	interruption	
	ļ		disclosure	Insiders acting deliberately:
	<u>.</u>	deliberate	modification	
network			loss, destruction	
			interruption	
			disclosure	Outsiders acting accidentally:
		accidental	modification	
	-		loss, destruction	
	outside		interruption	
			disclosure	Outsiders acting deliberately:
		deliberate	modification	
			loss, destruction	
			interruption	

hreat Con	text				Human Actors Usin Step 15	g Network A	Acces						
СРТ	Mot	ive			History								
How strong the actor's motive?		How confident are you in this estimate?			How often has this threat occurred in the past?	How accure are the date							
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 inyears								
					times in years								
					times in years								
					times in years								
					times in years								
					times in years								

Step 16

Iuman Actors Using Network A	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.	5	
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

	Activity S2.3
Step 12	Complete the threat tree for <i>human actors using physical access</i> . 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 <i>Threat Translation Guide</i> (see pp. 64-67 of this workbook).
Step 13	Record specific examples of threat actors on the <i>Risk Profile worksheet</i> for each applicable actor-motive combination.
C4 14	Decord the strongth of the motion for deliberate throats due to home or other Alexander
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.

ors Using l	Physical A	Access					Basic	Risk	Profile
_				Step 2	22				
	Thr	eat			1	Impact	Values	;	
			lity of a threat to						ea?
Access	Actor	Motive	Outcome						
				Reputation	Financial	Productivity	Fines	Safety	Other
			disclosure						
		accidental	modification						
			loss, destruction						
	inside	-	interruption						
_			disclosure						
	<u> </u>	deliberate	modification						
physical			loss, destruction						
			interruption						
			disclosure						
		accidental	modification						
			loss, destruction						
	outside	_	interruption						
			disclosure						
		deliberate	modification						
			loss, destruction						
			interruption						
֡	ranches is th lark these bro f the remaini ty of a threat Access	The granches is there a non-notark these branches on the fifthe remaining branches by of a threat to the asset? Access Actor inside physical	fark these branches on the tree. If the remaining branches is there a negli ty of a threat to the asset? Do not mark the Access Actor Motive accidental inside physical outside outside	Threat ranches is there a non-negligible possibility of a threat to lark these branches on the tree. f the remaining branches is there a negligible possibility or ty of a threat to the asset? Do not mark these branches. Access Actor Motive Outcome disclosure	Threat ranches is there a non-negligible possibility of a threat to fark these branches on the tree. If the remaining branches is there a negligible possibility or ty of a threat to the asset? Do not mark these branches. Access Actor Motive Outcome disclosure accidental modification loss, destruction interruption disclosure deliberate modification physical loss, destruction interruption disclosure accidental modification loss, destruction interruption disclosure deliberate modification loss, destruction interruption disclosure accidental modification loss, destruction interruption outside modification loss, destruction interruption disclosure deliberate modification loss, destruction loss, destruction interruption disclosure deliberate modification loss, destruction loss, destruction loss, destruction	Threat reanches is there a non-negligible possibility of a threat to lark these branches on the tree. If the remaining branches is there a negligible possibility or lark these branches. Access Actor Motive Outcome disclosure	Threat Threat Taraches is there a non-negligible possibility of a threat to lark these branches on the tree. Impact What is the potential organization in each organization i	Threat Threat Transches is there a non-negligible possibility of a threat to that these branches on the tree. Impact Values What is the potential impact or ganization in each application of a threat to the asset? Do not mark these branches. Access Actor Motive Outcome disclosure accidental modification inside loss, destruction interruption disclosure deliberate modification physical loss, destruction interruption disclosure deliberate modification loss, destruction interruption disclosure deliberate modification loss, destruction disclosure deliberate modification loss, destruction interruption disclosure deliberate modification loss, destruction loss, destruction	Threat ranches is there a non-negligible possibility of a threat to fark these branches on the tree. Impact Values What is the potential impact on the organization in each applicable are sy of a threat to the asset? Do not mark these branches. Access Actor Motive Outcome disclosure accidental modification loss, destruction interruption disclosure accidental modification physical loss, destruction interruption disclosure accidental modification loss, destruction interruption disclosure accidental modification loss, destruction interruption disclosure accidental modification loss, destruction loss, destruction interruption disclosure disclosure accidental modification loss, destruction

Basic R	Risk Pr	ofile	e										H	uma	n A	ctor	s Us	ing P	hysic	al A	ccess
Step 24				Step	26														Ste	27	
Pr How likel occur in t confident estimate?	the future are you	threa e? H	ow	Wha	it is th	e stoj	plight	t stati		y Pra h seci				rea?					Who app add	approaties yet is yet yet is yet yet is yet yet is yet is yet yet is yet	our for g
Value	Confi	iden	ce		S	Strate	egic						Ope	ratio	nal						
	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 Cutrl	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

an Actors Using	r nysical	Access		Threat Con
				Threat Actors
				Which actors pose the biggest threats to this system via physical means?
			disclosure	Insiders acting accidentally:
		accidental	-	
			loss, destruction	
	inside	<u> </u> 	interruption	
			disclosure	Insiders acting deliberately:
		deliberate	modification	
physical			loss, destruction	
			interruption	
			disclosure	Outsiders acting accidentally:
		accidental	modification	
			loss, destruction	
	outside	<u>.</u>	interruption	
			disclosure	Outsiders acting deliberately:
		deliberate	modification	, ,
			loss, destruction	
			interruption	

	t Cont	ext	_			Human Actors Usin	g Phys	ical	Acces
Motive					Step 15 History				
How strong is the actor's are you in this estimate?			you in		How often has this threat occurred in the past?		accui he dai		
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			

uman Actors Using Physical	Access	Areas of Concer
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 Acce Give examples of how outsiders acting accidentally could use physical access to threaten this system.	ss	
Give examples of how		
outsiders acting deliberately could use physical access to threaten this system.		

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 <i>system problems</i> . 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 <i>Threat Translation Guide</i> (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 2	22				
	Threat				Impact	Values	5	
	is there a non-negligible possile branches on the tree.	bility of a threat to	What is the potential impact on the organization in each applicable area?			ra?		
	naining branches is there a neg reat to the asset? Do not mark							
Asset	Actor	Outcome						
			Reputation	Financial	Productivity	Fines	Safety	Other
		disclosure						
	software defects	modification						
		loss, destruction						
		interruption						
		disclosure						
	system crashes	modification						
		loss, destruction						
		interruption						
		disclosure						
	hardware defects	modification						
		loss, destruction						
		interruption						
		disclosure						
	malicious code	modification						
	(virus, worm, Trojan horse, back door)	loss, destruction						
		interruption						

Basic Risk Profile		Sys	tem 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?	Secur What is the stoplight status for ea	rity Practice Areas ach security practice area?	Approach What is your approach for addressing each risk?
Value Confidence	Strategic	Operational	
Very Somewhat Not At All	 Sec Training Sec Strategy Sec Mgmt Sec Policy & Reg Coll Sec Mgmt 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
	disclosure	times in years	
software defects	modification	times in years	
	loss, destruction	times in years	
	interruption	times in years	
	disclosure	times in years	
system crashes	modification	times in years	
	loss, destruction	times in years	
	interruption	times in years	
	disclosure	times in years	
hardware defects	s modification	times in years	
	loss, destruction	times in years	
	interruption	times in years	
	disclosure	times in years	
malicious code	modification	times in years	
(virus, worm, Tr horse, back door		times in years	
	interruption	times in years	
			_

Threat Context	System Problems
Notes	
What additional notes about each threat do you want t	to record?

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.	1	
Hardware Defects		
Give examples of how hardware defects could threaten this system.		
Maliaiana Cada		
Malicious Code Give examples of how malicious code could threated this system. (Consider viruses, worms, Trojan horses, back doors, others)	1	

Areas of Concern

Software Defects
2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3
System Crashes
Hardware Defects
Hardware Detects
Malicious Code

6 Risk Profile Worksheet for Systems - Other Problems

Phase 1
Process S2
Activity S2.3

Step 12	Complete the threat tree for <i>other problems</i> . 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 <i>Threat Translation Guide</i> (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.
1	

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 2	22				
		Threat		Impact Values					
		ere a non-negligible possibil unches on the tree.	ity of a threat to	ity of a threat to What is the potential impact on the organization in each applicable an					
		ng branches is there a neglig to the asset? Do not mark th							
Asset		Actor	Outcome						
				Reputation	Financial	Productivity	Fines	Safety	Other
			disclosure						
		power supply	modification						
		problems	loss, destruction						
			interruption						
	1		disclosure						
		telecommunications	modification						
		problems or unavailability	loss, destruction						
			interruption						
			disclosure						
		third-party problems	modification						
		or unavailability of third-party systems	loss, destruction						
			interruption						
			disclosure						
		natural disasters	modification						
		(e.g., flood, fire, tornado)	loss, destruction						
			interruption						

Basic Risk Pı	ofile														O	ther Pr	oblems
Step 24	Step 26						_								Step 2	27	
Probability How likely is the threat to occur in the future? How confident are you in your estimate?		What is	Security Practice Areas What is the stoplight status for each security practice area?						Approach What is your approach for addressing each risk?								
Value Conf	fidence		Strategic				Ope	ratio	nal								
Very	Somewhat Not At All	1. Sec Training 2. Sec Strateov	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
	-																ם נ
	-																
	-																ם נ
	-] []
	-																ם נ
	-																ם נ
	-																ם נ
	-																
	-																ם נ
	-																ם נ
	-																ם נ
	-																1
	-																1
	-																ם נ
	-																ם נ
	-																

Other Problem	ns			Threat Context
			Step 15	
			Histo	ory
			How often has this threat occurred in the past?	How accurate are the data?
				Very Somewhat Not At All
		disclosure	times in year	rs 🔲 🗀
	power supply	modification	times in year	rs 🔲 🗀
	problems	loss, destruction	times in year	rs 🔲 🗀 🔲
		interruption	times in year	rs 🔲 🗀
	_	disclosure	times in year	rs 🔲 🗀 🔲
	telecommunications	modification	times in year	rs
	problems or unavailability	loss, destruction	times in year	rs 🔲 🗀 🗀
		interruption	times in year	rs 🔲 🗀 🗀
		disclosure	times in year	rs 🔲 🗆 🗆
	third-party problems	modification	times in year	rs 🔲 🗀 🗀
	or unavailability of third-party systems	loss, destruction	times in year	rs 🔲 🗀
		interruption	times in year	rs 🔲 🗀 🗀
		disclosure	times in year	rs
	natural disasters	modification	times in year	rs 🔲 🗆 🗆
	(e.g., flood, fire, tornado)	loss, destruction	times in year	rs 🔲 🗀
		interruption	times in year	rs 🔲 🗀 🗀

Threat Context	Other Problems
Notes	
What additional notes about each threat do you want to	record?

Other Problems		Areas of Concern
Power Supply Problem	ıs	
Give examples of how <i>p</i> supply problems could threaten this system.	ower	
Telecommunications P	roblems	
Give examples of how telecommunications processed threaten this system		
Third-Party Problems		
Give examples of how the party problems could that this system.		
Natural Disasters		
Give examples of how natural disasters could threaten this system.		

Areas of Concern

Power Supply Problems
11.0
Telecommunications Problems
Telecommunications 1100iems
Third-Party Problems
Natural Disasters

Other Problems	(cont.)				Basic	Risk	Profile
Step 12			Step 22				
the asset? Mark th	Threat es is there a non-negligible po nese branches on the tree.		Impact Values What is the potential impact on the organization in each applicable area.				
	remaining branches is there a threat to the asset? Do not mo						
Asset	Actor	Outcome					
			Reputation Financial	Productivity	Fines	Safety	Other
		disclosure					
	physical configuration	on modification					
	or arrangement of buildings, offices, or	loss, destruction					
	equipment	interruption					
		disclosure					
		modification					
		loss, destruction					
		interruption					
		disclosure					
		modification					
		loss, destruction					
		interruption					
		disclosure					
		modification					
		loss, destruction					
		interruption					
		L					

Basic Risk Profile	Г	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?	Security Practice An What is the stoplight status for each security practice.	
Value Confidence	Strategic	Operational
Very Somewhat Not At All	 Sec Training Sec Strategy Sec Mgmt Sec Policy & Reg Coll Sec Mgmt Cont Planning Phys Acc Cntrl Monitor Phys Sec Sec R. Not Mant 	9. Sys & Net ingine 10. Monitor IT Sec 11. Authen & Auth 12. Vul Mgmt 13. Encryption 14. Sec Arch & Des 15. Incident Mgmt Accept Defer Mitigate

Other Prob	lems (cont.)				Thr	eat C	Contex	t
			Step 15					
				History				
			How often has this the occurred in the past?	How are t				
					Very	Somewhat	Not At All	
		disclosure	times in	years				
	physical configuration	modification	times in	years				
	or arrangement of buildings, offices, or	loss, destruction	times in	years				
	equipment	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 we	ant to record?
	,

Other Problems (cont.)		Areas of Concern
Physical Configuration I	Problems	
Give examples of how physical configuration of buildings, offices, or equipment could threaten system.	his	
		7
Give examples of how		
could threaten this system		
Give examples of how could threaten this system		
]
Give examples of how		
could threaten this system		

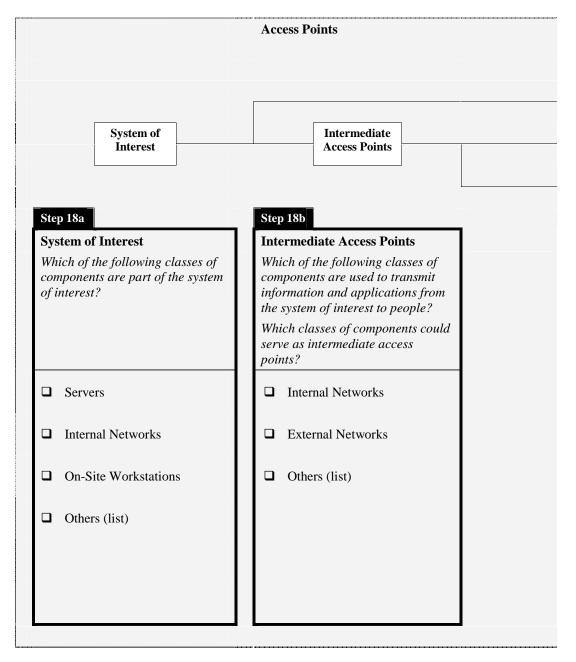
Areas of Concern	
	Physical Configuration Problems

Phase 2

7 Network Access Paths Worksheet

	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.

System of Interest What system or systems are most closely related to the critical asset?



Note: When you select a key class of components, make sure that you also document any relevant subclasses or specific examples when appropriate.

	Access Points	
System Access by People	Data Storage Locations	Other Systems/ Components
C4 10-	C4 10.1	
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.	Data Storage Locations On which classes of components is information from the system of interest stored for backup purposes?	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?
□ On-Site Workstations□ Laptops	☐ Storage Devices ☐ Others (list)	
□ PDAs/Wireless Components	G Oulers (list)	-
☐ Home/External Workstations		
☐ Others (list)		

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:

Source of Threat	Page
Human actors using network access	60-63
Human actors using physical access	64-67
System problems	68-71
Other problems	72-77

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.

	s Using Networ	-	No.41	0-4:
Asset	Access	Actor	Motive	Outcome
	. 1			
	network			
				disclosure
			accidental	modification
				loss, destruction
		outside		interruption
		L		<u> </u>
				disclosure
				disclosure
			deliberate	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 crashe 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.

		accidental	disclosure modification loss, destruction
		accidental	modification
		accidental	modification
		accidental	
		accidental	
			loss, destruction
			loss, destruction
			į
	inside		interruption
			disclosure
			disclosure
		1.17	1:6-
		denberate	modification
physical			loss, destruction
			interruption
	physical	physical	physical

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.

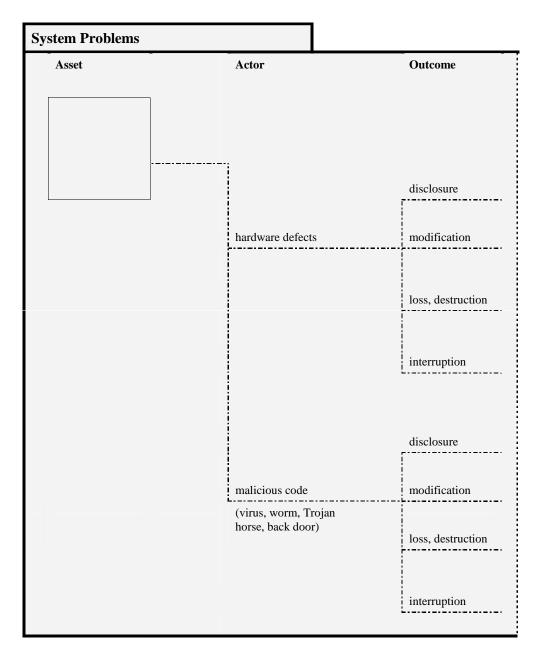
Asset	Access	Actor	Motive	Outcome
	physical			
	1 3			
				disclosure
			accidental	modification
				loss, destruction
		outside		interruption
				disclosure
			deliberate	modification
				loss, destruction
				interruption

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.

Asset	Actor	Outcome
		disclosure
	software defects	modification
		loss, destruction
		interruption
		disclosure
	system crashes	modification
		loss, destruction
		interruption

^{*} 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	An email server crashes, resulting in interruption of user access to email.



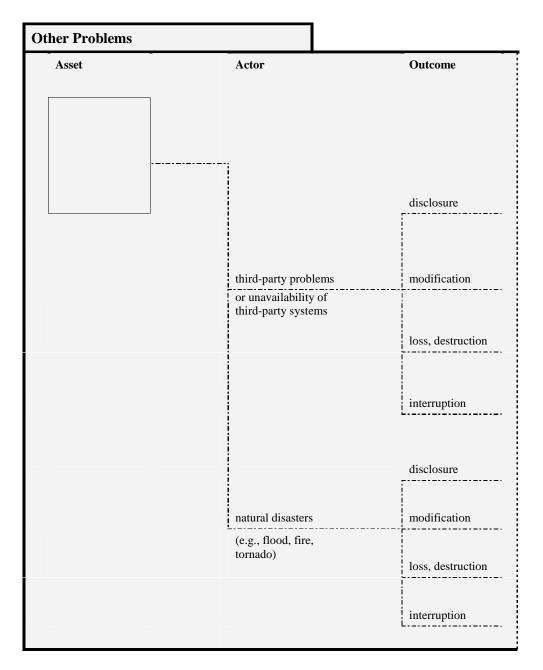
^{*} Blank lines indicate unusual or extremely rare possibilities.

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	A back door on a system enables unauthorized people to
horse, back door) that enables unauthorized parties to view information.	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.

Other Problems		
Asset	Actor	Outcome
		disclosure
	power supply	modification
	problems	loss, destruction
		interruption
		disclosure
	telecommunications	modification
	problems or unavailability	loss, destruction
		interruption

^{*} 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.	



^{*} 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.

Other Problems (con	nt.)	
Asset	Actor	Outcome
		disclosure
	physical configuration	modification
	or arrangement of buildings, offices, or equipment	loss, destruction
		interruption
		disclosure
		modification
		loss, destruction
		interruption

^{*} 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				
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.								
1.	AGENCY USE ONLY	2. REPORT DATE		3. REPORT	TYPE AND DATES COVERED			
	(Leave Blank)	January 2005		Final				
4.	. TITLE AND SUBTITLE			5. FUNDING NUMBERS				
	•	ation Guide, Version 1.0, Volum	ne 6	F19628-00-C-0003				
6.	AUTHOR(S)							
		udrey Dorofee, James Stevens,	Carol Woody					
7.	PERFORMING ORGANIZATION I	,,		8. PERFORMING ORGANIZATION				
	Software Engineering			REPORT NUMBER				
	Carnegie Mellon University Pittsburgh, PA 15213			CMU/SEI-2003-HB-003				
9.	•	ENCY NAME(S) AND ADDRESS(ES)	_	10. SPONSOR	RING/MONITORING AGENCY			
	HQ ESC/XPK			REPORT	NUMBER			
	5 Eglin Street	704.044						
	Hanscom AFB, MA 01	/31-2116						
11.	SUPPLEMENTARY NOTES							
12A	DISTRIBUTION/AVAILABILITY S			12B DISTRIBUTION CODE				
	Unclassified/Unlimited, DTIC, NTIS							
13.	ABSTRACT (MAXIMUM 200 WO	•						
		cal Threat, Asset, and Vulnerab						
		sment and planning technique fo						
		om an organization assume res						
	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	it will be able to colladet all deti-	vidos by itsell.	15. NUMBER OF PAGES				
	information security, risk management, OCTAVE		78					
16	PRICE CODE	on management, OOTAVE		,,,				
10. The cost								
17.	SECURITY CLASSIFICATION	18. SECURITY CLASSIFICATION OF	19. SECURITY CLASSIFICATION OF 20. LIMITATION OF ABSTRACT		20. LIMITATION OF ABSTRACT			
	OF REPORT	THIS PAGE	ABSTRACT UL					
1100	Unclassified	Unclassified	Unclassified					

NSN 7540-01-280-5500

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