

Carnegie Mellon
Software Engineering Institute

OCTAVE[®]-S Implementation Guide, Version 1.0

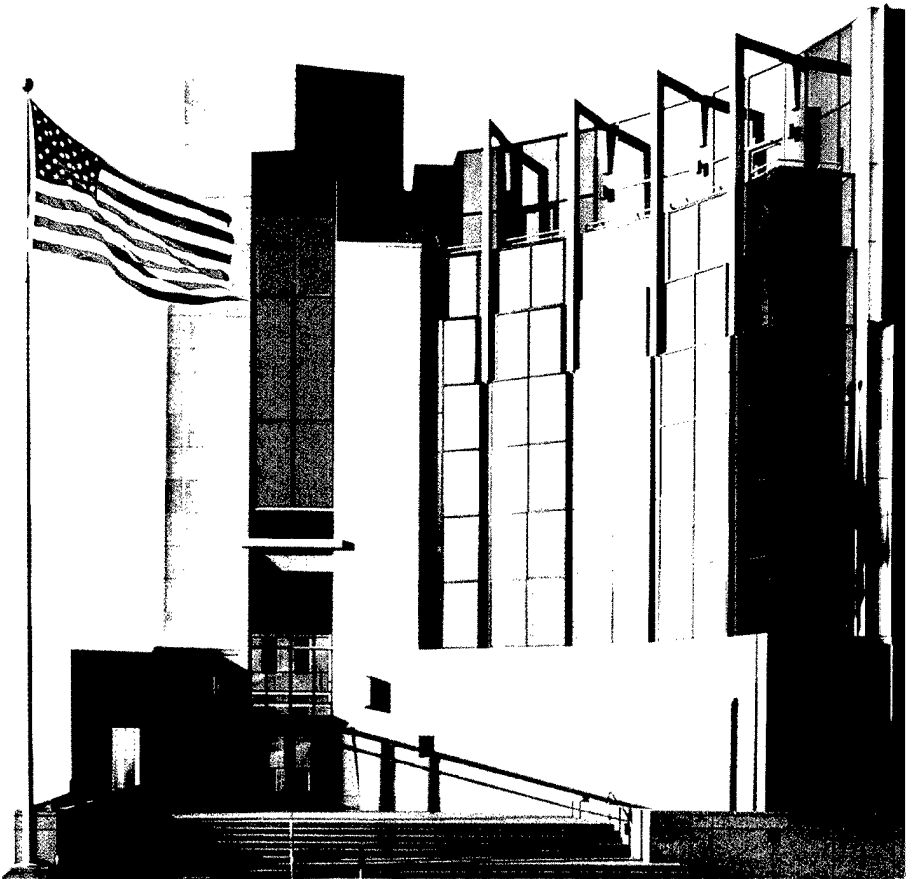
Volume 4: Organizational Worksheets

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

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

Unlimited distribution subject to the copyright.

20050322 126

This report was prepared for the

SEI Joint Program Office
ESC/XPX
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, XPX

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.

NO WARRANTY

® 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.

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>).

Table of Contents

About This Document..... v

Abstract..... vii

1 Introduction 1

2 Impact Evaluation Criteria Worksheet 5

3 Asset Identification Worksheet 19

4 Security Practices Worksheet 29

5 Critical Asset Selection Worksheet..... 61

6 Infrastructure Review Worksheet..... 65

7 Probability Evaluation Criteria Worksheet 71

List of Tables

Table 1: Worksheets Provided in This Workbook 1

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 EvaluationSM (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 EvaluationSM (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 <ul style="list-style-type: none"> what your organization is currently doing well in this area (security practices) what your organization is currently <i>not</i> 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	<p>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.</p> <p>Finally, document any additional context relevant to your infrastructure review.</p>	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 I
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
<i>Reputation</i>	Reputation is minimally affected; little or no effort or expense is required to recover.
<i>Customer Loss</i>	Less than _____% reduction in customers due to loss of confidence
<i>Other:</i>	
<i>Other:</i>	

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
<i>Operating Costs</i>	Increase of less than _____% in yearly operating costs
<i>Revenue Loss</i>	Less than _____% yearly revenue loss
<i>One-Time Financial Loss</i>	One-time financial cost of less than \$ _____
<i>Other:</i>	

Impact Evaluation Criteria Worksheet

		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
<i>Staff Hours</i>	Staff work hours are increased by less than _____% for _____ to _____ day(s).
<i>Other:</i>	
<i>Other:</i>	
<i>Other:</i>	

Impact Evaluation Criteria Worksheet

		Productivity
Medium Impact	High Impact	
<p>Staff work hours are increased between _____% and _____% for _____ to _____ day(s).</p>	<p>Staff work hours are increased by greater than _____% for _____ to _____ day(s).</p>	

Step 1	
Safety/Health	
Impact Type	Low Impact
<i>Life</i>	No loss or significant threat to customers' or staff members' lives
<i>Health</i>	Minimal, immediately treatable degradation in customers' or staff members' health with recovery within four days
<i>Safety</i>	Safety questioned
<i>Other:</i>	

Impact Evaluation Criteria Worksheet

		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
<i>Fines</i>	Fines less than \$_____ are levied.
<i>Lawsuits</i>	Non-frivolous lawsuit or lawsuits less than \$_____ are filed against the organization, or frivolous lawsuit(s) are filed against the organization.
<i>Investigations</i>	No queries from government or other investigative organizations
<i>Other:</i>	

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:	

Impact Evaluation Criteria Worksheet

		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
<i>What systems do people in your organization need to perform their jobs?</i>	<i>What information do people in your organization need to perform their jobs?</i>

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

Step 2

Information, Systems, and Applications (cont.)	
System	Information
<i>What systems do people in your organization need to perform their jobs?</i>	<i>What information do people in your organization need to perform their jobs?</i>

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

Step 2

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

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

Step 2

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

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

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 <ul style="list-style-type: none">• what your organization is currently doing well in this area (security practices)• what your organization is currently <i>not</i> 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 <ul style="list-style-type: none"> • 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

What is your organization currently doing well in this area?	What is your organization currently <i>not</i> doing well in this area?

Step 4

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 <i>not</i> 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 <ul style="list-style-type: none"> • 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	Step 4
What is your organization currently doing well in this area?	What is your organization currently <i>not</i> doing well in this area?
How effectively is your organization implementing the practices in this area?	
<input type="checkbox"/> Red <input type="checkbox"/> Yellow <input type="checkbox"/> Green <input type="checkbox"/> 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 <ul style="list-style-type: none"> • 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 <i>not</i> doing well in this area?
How effectively is your organization implementing the practices in this area?	
<input type="checkbox"/> Red <input type="checkbox"/> Yellow <input type="checkbox"/> Green <input type="checkbox"/> Not Applicable	

5. Collaborative Security Management

Step 3a

Statement	To what extent is this statement reflected in your organization?
<p>The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including</p> <ul style="list-style-type: none"> • protecting information belonging to other organizations • understanding the security policies and procedures of external organizations • ending access to information by terminated external personnel 	<p>Very Much Somewhat Not At All Don't Know</p>
<p>The organization documents information protection requirements and explicitly communicates them to all appropriate third parties.</p>	<p>Very Much Somewhat Not At All Don't Know</p>
<p>The organization has formal mechanisms for verifying that all third-party organizations, outsourced security services, mechanisms, and technologies meet its needs and requirements.</p>	<p>Very Much Somewhat Not At All Don't Know</p>
<p>The organization has policies and procedures for collaborating with all third-party organizations that</p> <ul style="list-style-type: none"> • provide security awareness and training services • develop security policies for the organization • develop contingency plans for the organization 	<p>Very Much Somewhat Not At All Don't Know</p>

5. Collaborative Security Management

Step 3b

What is your organization currently doing well in this area?	What is your organization currently <i>not</i> doing well in this area?

Step 4

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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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

What is your organization currently doing well in this area?	What is your organization currently <i>not</i> doing well in this area?

Step 4

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?
<i>If staff from your organization is responsible for this area:</i>	
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
<i>If staff from a third party is responsible for this area:</i>	
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 <i>not</i> doing well in this area?	How effectively is your organization implementing the practices in this area?
		<input type="checkbox"/> Red <input type="checkbox"/> Yellow <input type="checkbox"/> Green <input type="checkbox"/> Not Applicable

8. Monitoring and Auditing Physical Security

Step 3a

Statement	To what extent is this statement reflected in your organization?
<i>If staff from your organization is responsible for this area:</i>	
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
<i>If staff from a third party is responsible for this area:</i>	
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

What is your organization currently doing well in this area?	What is your organization currently <i>not</i> doing well in this area?

Step 4

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?			
<i>If staff from your organization is responsible for this area:</i>				
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. <ul style="list-style-type: none"> • 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
<i>If staff from a third party is responsible for this area:</i>				
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

What is your organization currently doing well in this area?	What is your organization currently <i>not</i> doing well in this area?

Step 4

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?
<p><i>If staff from your organization is responsible for this area:</i></p> <p>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.</p>	Very Much Somewhat Not At All Don't Know
<p>Firewall and other security components are periodically audited for compliance with policy.</p>	Very Much Somewhat Not At All Don't Know
<p><i>If staff from a third party is responsible for this area:</i></p> <p>The organization's requirements for monitoring information technology security are formally communicated to all contractors and service providers that monitor systems and networks.</p>	Very Much Somewhat Not At All Don't Know
<p>The organization formally verifies that contractors and service providers have met the requirements for monitoring information technology security.</p>	Very Much Somewhat Not At All Don't Know

10. Monitoring and Auditing IT Security

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

11. Authentication and Authorization

Step 3a

Statement	To what extent is this statement reflected in your organization?
<p><i>If staff from your organization is responsible for this area:</i></p> <p>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.</p>	<p>Very Much Somewhat Not At All Don't Know</p>
<p>There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.</p>	<p>Very Much Somewhat Not At All Don't Know</p>
<p>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.</p>	<p>Very Much Somewhat Not At All Don't Know</p>
<p><i>If staff from a third party is responsible for this area:</i></p> <p>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.</p>	<p>Very Much Somewhat Not At All Don't Know</p>
<p>The organization formally verifies that contractors and service providers have met the requirements for authentication and authorization.</p>	<p>Very Much Somewhat Not At All Don't Know</p>

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?
<p><i>If staff from your organization is responsible for this area:</i></p> <p>There is a documented set of procedures for managing vulnerabilities, including</p> <ul style="list-style-type: none"> • 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 	<p>Very Much Somewhat Not At All Don't Know</p>
<p>Vulnerability management procedures are followed and are periodically reviewed and updated.</p>	<p>Very Much Somewhat Not At All Don't Know</p>
<p>Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.</p>	<p>Very Much Somewhat Not At All Don't Know</p>
<p><i>If staff from a third party is responsible for this area:</i></p> <p>The organization's vulnerability management requirements are formally communicated to all contractors and service providers that manage technology vulnerabilities.</p>	<p>Very Much Somewhat Not At All Don't Know</p>
<p>The organization formally verifies that contractors and service providers have met the requirements for vulnerability management.</p>	<p>Very Much Somewhat Not At All Don't Know</p>

12. Vulnerability Management

Step 3b

What is your organization currently doing well in this area?	What is your organization currently <i>not</i> 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?
<p><i>If staff from your organization is responsible for this area:</i></p> <p>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).</p>	<p>Very Much Somewhat Not At All Don't Know</p>
<p>Encrypted protocols are used when remotely managing systems, routers, and firewalls.</p>	<p>Very Much Somewhat Not At All Don't Know</p>
<p><i>If staff from a third party is responsible for this area:</i></p> <p>The organization's requirements for protecting sensitive information are formally communicated to all contractors and service providers that provide encryption technologies.</p>	<p>Very Much Somewhat Not At All Don't Know</p>
<p>The organization formally verifies that contractors and service providers have met the requirements for implementing encryption technologies.</p>	<p>Very Much Somewhat Not At All Don't Know</p>

13. Encryption

Step 3b	Step 4
What is your organization currently doing well in this area?	What is your organization currently <i>not</i> doing well in this area?
How effectively is your organization implementing the practices in this area?	
<input type="checkbox"/> Red <input type="checkbox"/> Yellow <input type="checkbox"/> Green <input type="checkbox"/> Not Applicable	

14. Security Architecture and Design

Step 3a

Statement	To what extent is this statement reflected in your organization?
<p><i>If staff from your organization is responsible for this area:</i></p> <p>System architecture and design for new and revised systems include considerations for</p> <ul style="list-style-type: none"> • security strategies, policies, and procedures • history of security compromises • results of security risk assessments 	<p>Very Much Somewhat Not At All Don't Know</p>
<p>The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.</p>	<p>Very Much Somewhat Not At All Don't Know</p>
<p><i>If staff from a third party is responsible for this area:</i></p> <p>The organization's security-related requirements are formally communicated to all contractors and service providers that design systems and networks.</p>	<p>Very Much Somewhat Not At All Don't Know</p>
<p>The organization formally verifies that contractors and service providers have met the requirements for security architecture and design.</p>	<p>Very Much Somewhat Not At All Don't Know</p>

14. Security Architecture and Design

Step 3b

What is your organization currently doing well in this area?	What is your organization currently <i>not</i> doing well in this area?
---	--

--	--

Step 4

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?
<i>If staff from your organization is responsible for this area:</i>	
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
<i>If staff from a third party is responsible for this area:</i>	
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

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

5 Critical Asset Selection Worksheet

Phase I
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 <i>Which classes of components are related to one or more critical assets?</i>	Critical Assets <i>Which critical assets are related to each class?</i>	Responsibility <i>Who is responsible for maintaining and securing each class of components?</i>																												
<i>(Document any relevant subclasses or specific examples when appropriate.)</i>	<table border="1"> <tr> <td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>1.</td><td>2.</td><td>3.</td><td>4.</td><td>5.</td> </tr> </table>						1.	2.	3.	4.	5.																			
1.	2.	3.	4.	5.																										
<table border="1"> <tr><td>Servers</td></tr> <tr><td></td></tr> <tr><td></td></tr> <tr><td></td></tr> </table>	Servers				<table border="1"> <tr><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td></tr> </table>																					<table border="1"> <tr><td></td></tr> <tr><td></td></tr> <tr><td></td></tr> <tr><td></td></tr> </table>				
Servers																														
<table border="1"> <tr><td>Internal Networks</td></tr> <tr><td></td></tr> <tr><td></td></tr> <tr><td></td></tr> </table>	Internal Networks				<table border="1"> <tr><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td></tr> </table>																					<table border="1"> <tr><td></td></tr> <tr><td></td></tr> <tr><td></td></tr> <tr><td></td></tr> </table>				
Internal Networks																														
<table border="1"> <tr><td>On-Site Workstations</td></tr> <tr><td></td></tr> <tr><td></td></tr> <tr><td></td></tr> </table>	On-Site Workstations				<table border="1"> <tr><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td></tr> </table>																					<table border="1"> <tr><td></td></tr> <tr><td></td></tr> <tr><td></td></tr> <tr><td></td></tr> </table>				
On-Site Workstations																														
<table border="1"> <tr><td>Laptops</td></tr> <tr><td></td></tr> <tr><td></td></tr> <tr><td></td></tr> </table>	Laptops				<table border="1"> <tr><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td></tr> </table>																					<table border="1"> <tr><td></td></tr> <tr><td></td></tr> <tr><td></td></tr> <tr><td></td></tr> </table>				
Laptops																														
<table border="1"> <tr><td>PDAs/Wireless Components</td></tr> <tr><td></td></tr> <tr><td></td></tr> <tr><td></td></tr> </table>	PDAs/Wireless Components				<table border="1"> <tr><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td></tr> </table>																					<table border="1"> <tr><td></td></tr> <tr><td></td></tr> <tr><td></td></tr> <tr><td></td></tr> </table>				
PDAs/Wireless Components																														

Step 21

Protection				How do you know?		
<i>To what extent is security considered when configuring and maintaining each class of components?</i>				<i>How do you know?</i>		
Very Much	Somewhat	Not At All	Don't Know	Formal Techniques	Informal Means	Other

Notes/Issues
<i>What additional information do you want to record?</i>

Servers

----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

Internal Networks

----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

On-Site Workstations

----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

Laptops

----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

PDAs/Wireless Components

----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

Step 21

Protection			
<i>To what extent is security considered when configuring and maintaining each class of components?</i>		<i>How do you know?</i>	
Very Much	Somewhat	Not At All	Don't Know
		Formal Techniques	Informal Means
		Other	

Notes/Issues
<i>What additional information do you want to record?</i>

Other Systems

----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

Storage Devices

----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

External Networks

----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

Home/External Workstations

----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

Other _____

----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
----- ----- <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

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 PAGEForm Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave Blank)		2. REPORT DATE January 2005	3. REPORT TYPE AND DATES COVERED Final	
4. TITLE AND SUBTITLE OCTAVE-S Implementation Guide, Version 1.0, Volume 4			5. FUNDING NUMBERS F19628-00-C-0003	
6. AUTHOR(S) Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213			8. PERFORMING ORGANIZATION REPORT NUMBER CMU/SEI-2003-HB-003	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12A DISTRIBUTION/AVAILABILITY STATEMENT Unclassified/Unlimited, DTIC, NTIS			12B DISTRIBUTION CODE	
13. ABSTRACT (MAXIMUM 200 WORDS) The Operationally Critical Threat, Asset, and Vulnerability Evaluation SM (OCTAVE [®]) approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization's personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks. To conduct OCTAVE-S effectively, the team must have broad knowledge of the organization's business and security processes, so it will be able to conduct all activities by itself.				
14. SUBJECT TERMS information security, risk management, OCTAVE			15. NUMBER OF PAGES 74	
16. PRICE CODE				
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	