

# **Applying OCTAVE: Practitioners Report**

## **Author**

Carol Woody, PhD

## **Contributors**

Johnathan Coleman

Michael Fancher

Carol Myers

Lisa Young

*May 2006*

**Networked Systems Survivability**

Unlimited distribution subject to the copyright.

**Technical Note**  
CMU/SEI-2006-TN-010

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 2006 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 FA8721-05-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>).

---

# Contents

<b>Abstract</b> .....	<b>vii</b>
<b>1 Introduction</b> .....	<b>1</b>
<b>2 About OCTAVE</b> .....	<b>2</b>
2.1 Security Risk Methodology Classification .....	2
2.2 Brief Background of the OCTAVE Approach.....	4
<b>3 Applying OCTAVE to an Organization</b> .....	<b>6</b>
3.1 Evaluating the OCTAVE Catalog of Practices.....	7
3.2 Evaluating the Information Gathering Approach .....	7
3.3 Evaluating the Needs of Decision-Makers and Context-Sensitive Terminology .....	8
3.4 Evaluating the Range of Threats .....	9
3.5 Determining Relevant Evaluation Criteria.....	9
<b>4 OCTAVE in Practice</b> .....	<b>11</b>
4.1 Addressing HIPAA-Mandated Risk Assessments with OCTAVE .....	12
4.2 Enhancements to OCTAVE by the National Center for Manufacturing Sciences .....	16
4.3 Florida Tackles Enterprise Risk Management with OCTAVE and NIST SP 800-30.....	20
4.4 Paradise Valley Community College Tailored OCTAVE for Security Risk Management.....	25
4.5 Case Study: An Information Technology Security Risk Assessment for the Telescopes in Education Project at Paradise Valley Community College .....	27
<b>5 About the Contributors</b> .....	<b>31</b>
<b>Appendix A Timeline for OCTAVE in Practice</b> .....	<b>33</b>
<b>Appendix B NIST SP 800-30/OCTAVE Correlation</b> .....	<b>35</b>
<b>References</b> .....	<b>37</b>



---

## List of Figures

Figure 1: Risk Management Process Within the Organizational Context.....	2
Figure 2: Results of an Unbalanced Security Risk Management Process .....	4
Figure 3: Information Security Risk Evaluation Within an Information Security Risk Management Process .....	9
Figure 4: Generic High-Level Process Diagram .....	18
Figure 5: Example Asset Inventory and Critical Asset Identification for a Manufacturing Process.....	19



---

## List of Tables

Table 1:	Server Descriptions for PVACS .....	28
Table 2:	PVACS Business Process Risks .....	29
Table 3:	PVACS Security Risks.....	29
Table 4:	NIST SP 800-30/OCTAVE Method Correlation .....	35



---

## Abstract

The CERT Operationally Critical Threat, Asset, and Vulnerability Evaluation<sup>SM</sup> (OCTAVE<sup>®</sup>) method, an approach for managing information security risks, was designed to be sufficiently flexible for organizations to address unique and highly contextual analysis needs through tailoring capabilities. This document describes how OCTAVE has been used and tailored to fit a wide range of organizational risk assessment needs. Guidelines for successful tailoring, built on the reporting practitioners' successes, are provided to help organizations fit the OCTAVE approach to their specific domain and organizational needs. The range of applications demonstrates the flexibility of the OCTAVE approach and its value in addressing security risk management.

Readers should already be familiar with the general concepts of the OCTAVE approach.



---

# 1 Introduction

The CERT Operationally Critical Threat, Asset, and Vulnerability Evaluation<sup>SM</sup> (OCTAVE<sup>®</sup>) method, an approach for managing information security risks, has been successfully tailored to address a wide range of organizational domains and contexts. After a group of these experiences were analyzed, patterns of effective tailoring emerged that can help those evaluating the OCTAVE approach's applicability to their organizational needs. This technical note describes those patterns and includes examples from four different domains.

This technical note includes the following sections:

- Section 2 describes the value of a balanced approach to security risk management and the characteristics of the OCTAVE approach that support this balance.
- Section 3 provides general guidelines for tailoring the OCTAVE approach to fit the needs of a specific organizational domain and context.
- Section 4 describes the tailoring and use of the OCTAVE approach in four unique domains by contributors who are experts in their fields: healthcare, manufacturing, state and local government, and higher education. It also includes a case study for higher education.
- Section 5 provides information about the contributors who have shared their experiences for the benefit of others considering the OCTAVE approach. It has been a privilege to work with them in this effort.

---

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

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

---

## 2 About OCTAVE

### 2.1 Security Risk Methodology Classification

There are many standards, practices, and methods available for addressing information security risks. Selecting the right option(s) for an organization depends on the range of laws and regulations, organizational goals and objectives, and management practices and organizational policies that define the parameters within which the security risk management process must abide.

As shown in Figure 1, there are many methodologies that address individual parts of an organization's risk management needs. Organizations may look at what others within their domain have used as viable options, focusing on laws and regulations. Organizations may be mandated to apply specific standards to achieve regulatory compliance. In addition, an organization's size and financial resources help determine appropriate choices. For example, adoption of a general standard of due care, such as International Organization for Standardization (ISO) 17799, can be prohibitively costly and does not guarantee that the security issues of a specific organization have been addressed. Each organization must understand its risk and plan for appropriate protection.

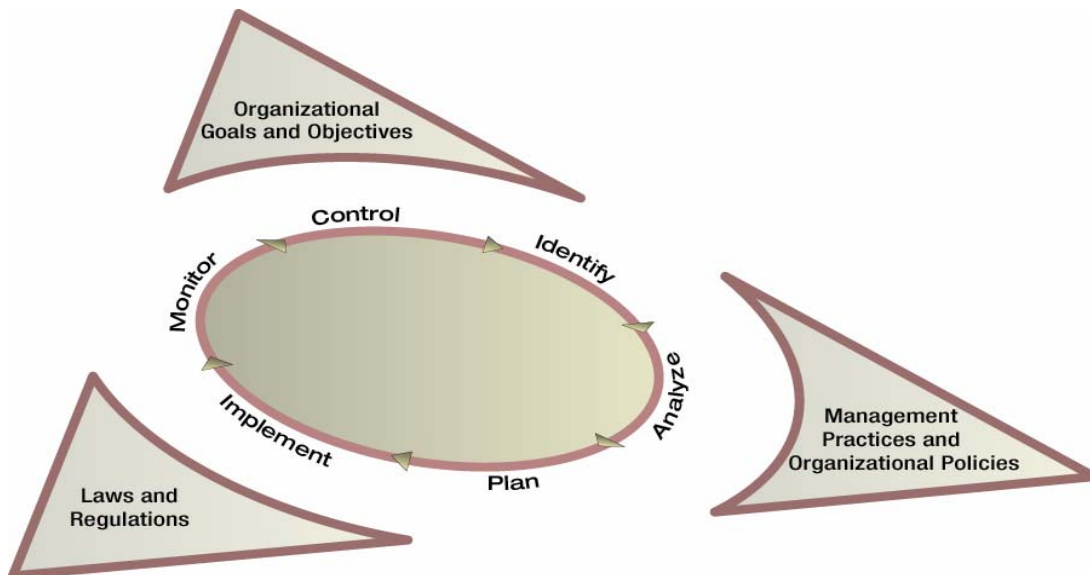


Figure 1: Risk Management Process Within the Organizational Context

An attempt to classify risk assessment methods was published by Sandia National Laboratories in 2004 [Campbell 2004]. Campbell and Stamp identified three categories: (1) temporal methodologies that focus on technology systems using actual tests, (2) comparative methodologies that concentrate on a specific standard, and (3) functional methodologies that balance the other two to apply tests and standards. OCTAVE is classified as a functional methodology. The strength of this methodology type is that specific threats, vulnerabilities, assets, and countermeasures important to the context of the organization are included.

Campbell and Stamp's classification approach identifies two factors—(1) knowledge of the methodology and (2) contextual knowledge—that must be balanced for the methodology to be applied successfully. It also defines who must lead the process [Campbell 2004]: experts lead when methodology knowledge is critical, and system owners lead when contextual knowledge is critical. OCTAVE is classified as mid-level and balances the two extremes. Some organizations apply OCTAVE unassisted, and others enlisted vendors to supplement their knowledge of security risk management.

The OCTAVE approach uses an asset-based information security risk assessment. Security risk is carefully considered based on the organizational and technology vulnerabilities that threaten a group of mission-critical assets. By considering more than just the technology vulnerabilities that a suite of tools can identify from an organization's hardware and software infrastructure, the OCTAVE approach addresses the following questions:<sup>1</sup>

- What assets require protection?
- What level of protection is needed?
- How might an asset be compromised?
- What is the impact if protection fails?

By using a balanced approach that blends technology considerations with organizational ones across a reasonable segment of the organization, an organization should be able to avoid overprotecting some areas while underprotecting others. Figure 2 (by David Biber) provides a humorous but frequently true depiction of the information security management in an organization that only considers one portion of the information security risk challenge.

---

<sup>1</sup> Dorofee, A. *Asset-Based Information Security Risk Assessments*, Cutter Consortium, *Enterprise Risk Management and Governance Executive Report*, Vol. 2, No. 6. Available for purchase online at <http://www.cutter.com>.



Figure 2: Results of an Unbalanced Security Risk Management Process

## 2.2 Brief Background of the OCTAVE Approach

The conceptual framework that formed the basis of the OCTAVE approach was published by the Software Engineering Institute (SEI) at Carnegie Mellon University in 1999 [Alberts 1999]. These concepts were formalized into the OCTAVE Criteria, published in 2001 [Alberts 2001a]. Working with the Telemedicine and Advanced Technology Research Center (TATRC), the SEI developed the OCTAVE method to apply the OCTAVE approach to the security compliance challenges faced by the U. S. Department of Defense (DoD) when the security compliance portion of the Health Insurance Portability and Accountability Act (HIPAA) was mandated. The OCTAVE method was released for public use in September 2001.

OCTAVE<sup>®</sup>-S was developed by SEI under the Technology Insertion, Demonstration, and Evaluation (TIDE) program (<http://www.sei.cmu.edu/tide/>) to apply the OCTAVE approach to small manufacturing organizations. It was released for public use in September 2003.

Guidelines for selecting the OCTAVE method or OCTAVE-S are included in a technical note published in August 2003 [Alberts 2003]. For the complete timeline of OCTAVE approach development, see Appendix A.

---

<sup>®</sup> OCTAVE-S is registered in the United States Patent and Trademark Office by Carnegie Mellon University.

The OCTAVE method and OCTAVE-S have been widely referenced by the international information security community. Between June 2003 and June 2005, the OCTAVE method was downloaded by more than 9,600 sources. During this same time frame, OCTAVE-S was downloaded by more than 4,700 sources. This group of potential users included private companies (50%), individuals (15%), academic institutions (15%), and government organizations (10%). On average, the OCTAVE Web site receives 5,000 visitors a month.

Familiarity with the OCTAVE approach will enhance understanding of this technical note. Two important sources of OCTAVE information are (1) the OCTAVE Web site (<http://www.cert.org/octave>) and (2) *Managing Information Security Risks: The OCTAVE Approach* [Alberts 2002].

---

### 3 Applying OCTAVE to an Organization

There are several key areas that must be linked to the organization's context and domain (e.g., healthcare or education) to effectively apply an OCTAVE-based methodology. The following key areas must be understood and the methodology may require tailoring for an appropriate fit:

- The catalog of security practices used to assess risk must address the regulatory and accepted security practices for the organizational domain.
- The ways in which risk assessment information is gathered must fit the organizational context.
- The documents produced as the methodology is used should be written for the organization's decision makers using the appropriate level of detail and context-specific terminology.
- The threats considered within the analysis steps must be consistent with those considered relevant to the organization.
- Evaluation criteria used to assess a risk's impact on the organization and to prioritize risks for mitigation considerations must be based on relevant organizational measures.

Sections 3.1 through 3.5 address the tailoring needs listed above in more detail. In addition, when applying an OCTAVE methodology—with or without tailoring—the following general guidelines are critical for embedding the organizational context into the OCTAVE approach. These guidelines should be considered as each execution of OCTAVE is planned:

- The analysis team should include individuals familiar with the organization and the OCTAVE approach. External resources may be the most appropriate OCTAVE source of this expertise if internal resources are not already trained. Tailoring requires participation by organizational and OCTAVE resources.
- The information sources included in the assessment do not need to be exhaustive, but they must provide a reasonably complete context. They should represent sufficient knowledge of the organization, the specific organizational areas selected for analysis, and the information assets selected for critical analysis.
- Information security management is a subset of organizational risk, and the organization may benefit from a coordinated range of assessment efforts that address enterprise risk management.

### 3.1 Evaluating the OCTAVE Catalog of Practices

Two types of review are required:

1. **Necessary Validation:** Is the catalog of practices (COP) used by the OCTAVE approach relevant to the organization?
2. **Sufficiency Validation:** Are any aspects of security regulation and practice that are critical to the organization missing from the catalog?

Begin with a review of OCTAVE COP sources [Alberts 2001b]. Because the OCTAVE COP was based on a reasonable set of good security practices applicable to the healthcare and manufacturing domains, experience has generally shown that the catalog is necessary, but it may not be sufficient. If a domain has well-defined security practices, map them to the OCTAVE COP to identify strengths and limitations. For a mapping between OCTAVE COP and National Institute of Standards and Technology Special Publication (NIST SP) 800-30, see Appendix B.

If a domain does not have well-defined security practices (e.g., education), appropriate practices can be developed by evaluating security events and problems relevant to the domain. Sources include domain-specific books and articles, general news publications, and technology publications such as the “SANS NewsBites” (<http://www.sans.org/newsletters>) and AIG National Union’s “Top Ten Tech Issues.”

For each critical event, the relevant security risk, consequence, and security practice can be assembled. Using this technique for K-12 schools and school districts yielded the following security practices that were not included in the OCTAVE COP [Woody 2004]:

- content blocking to filter pornography and limit access to inappropriate activities (e.g., gambling) and monitoring to minimize the impacts of censorship
- structured access to ensure privacy, accommodate device sharing, and control access rights
- regulatory compliance for the Children’s Online Privacy Protection Act (COPPA), application of copyright and licensing laws to digital media, and the USA PATRIOT Act
- acceptable educational uses to assign appropriate levels of responsibility to participants based on age level, allow appropriate organizational use of available digital content, and promote ethical behavior

### 3.2 Evaluating the Information Gathering Approach

The OCTAVE method includes organizational information gathering through workshops that include senior managers, operational managers, operational staff, and information technology (IT) staff. The implied organizational structure is hierarchical, and workshops can be top-down or bottom-up depending on the organization’s authority structure. Workshops are conducted by a team that bridges organizational lines so that information security issues are

addressed from an enterprise perspective. There is no set number of workshops that can be performed for an assessment: however, each workshop increases the volume of information that an analysis team must evaluate.

OCTAVE-S requires that the analysis team contains sufficient organizational knowledge to provide the enterprise perspective without additional information gathering steps. The methodology is streamlined for the less formal style of small organizations, and it assumes that the organization has a limited number of security experts participating in the process. The analysis team uses OCTAVE-S templates—comprised of standard text, selection boxes, and notes—to guide and document security discussions. Because the templates are so detailed, OCTAVE-S tailoring would be tedious and has not been reported to SEI.

Many different types of information gathering have been successfully applied. Web survey forms have been used to gather input from broadly disbursed organizational units and participants with unusual schedules who cannot easily attend workshops. Individual interviews have been conducted when workshop participation is not supported. While this allows in-depth discussions and ensures input from all participants, it extends the organizational information gathering and analysis activities. Therefore, the benefits should be clearly articulated to justify the additional time.

### **3.3 Evaluating the Needs of Decision-Makers and Context-Sensitive Terminology**

At the end of an evaluation, the analysis team proposes plans for addressing organizational strategic protection and mitigating priority risks for critical information assets. For OCTAVE-based evaluations, details are captured in a written report or presentation assembled for management review and acceptance; for OCTAVE-S, details are captured in completed templates.

As shown in Figure 3, additional effort is required within the organization to implement, monitor, and control the plans. Because these plans must be folded into the organization's context for improvements to occur, the analysis team should use terminology that is familiar to the decision makers. For planning and scoping purposes, these additional steps need to be identified in advance.

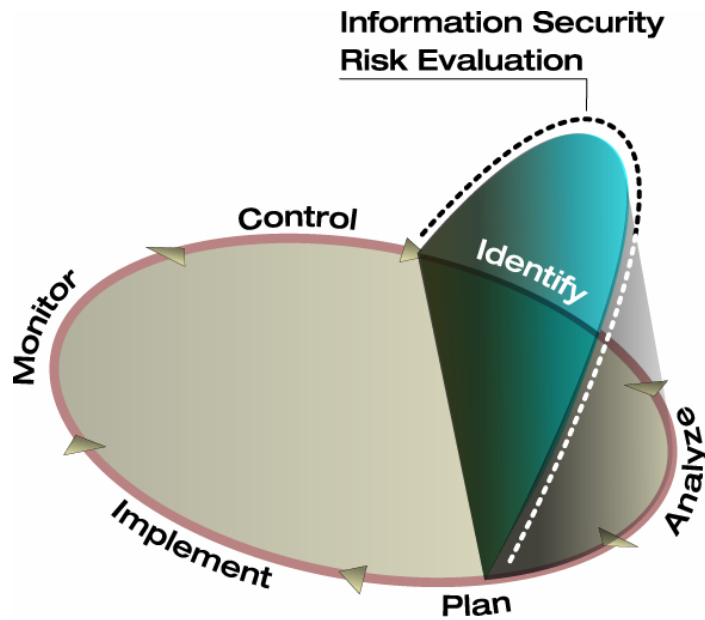


Figure 3: Information Security Risk Evaluation Within an Information Security Risk Management Process

### 3.4 Evaluating the Range of Threats

Both the OCTAVE method and OCTAVE-S incorporate a generic threat tree analysis technique [Alberts 2001c] that assembles threats into the following structure:

- threat access (e.g., network, physical, system, and so on)
- if applicable, threat actor (e.g., insider or outsider)
- if applicable, threat actor motive (e.g., deliberate or accidental)
- threat outcome (disclosure, modification, loss, destruction, or interruption)

There are unique groups of actors who may be trusted outsiders (e.g., consultants, students, and vendors providing on-site support). If these groups are sufficiently large, the analysis team may choose to consider their actions separately and modify the generic threat trees.

### 3.5 Determining Relevant Evaluation Criteria

The OCTAVE method and OCTAVE-S use the following general criteria to identify the potential impact of a security threat:

- loss of reputation and/or customer confidence
- life and health of customers
- productivity
- fines and legal penalties
- financial loss

Not all organizations are prepared to address risks for each general criterion. For example, life and health of customers is very relevant to a medical organization, but it is less important to a financial institution, which may decide to drop the criterion. For Kindergarten through 12<sup>th</sup> grade (K-12) schools and school districts, none of the general criteria proved relevant. For this domain, the primary concern is lost of teaching moment opportunities. Criteria were adjusted to reflect this critical evaluation type, and threats were evaluated based on the number of possible classroom hours jeopardized [Woody 2004].

---

## 4 OCTAVE in Practice

This section describes ways in which the OCTAVE approach was successfully tailored to meet the contextual issues of organizations in four different domains (healthcare, manufacturing, state government, and higher education). Where available, the specific methodology that was used, the OCTAVE method or OCTAVE-S, is specified. This material was provided by individuals who are actively applying the OCTAVE approach to address their security risk management challenges. Each contributor responded to the following questions to help you understand how using the OCTAVE approach could enhance your organization's security risk management:

- What made OCTAVE the right choice for the basis of risk management?
- What makes this use of OCTAVE unique?
- What makes this a success story?
- What lessons learned were identified to allow for improvement the next time?

In Section 4.1, Johnathan Coleman addresses HIPAA-mandated risk assessments using the OCTAVE method. He shares the steps required to apply security risk management to address healthcare regulatory requirements as implemented within the DoD.

In Section 4.2, Michael Fancher describes enhancements to the OCTAVE approach by the National Center for Manufacturing Sciences. He shares techniques, applied to a range of organizations, that were used to integrate security risk management into manufacturing practices.

In Section 4.3, Lisa Young reports on how Florida tackles enterprise risk management (ERM) with the OCTAVE method and NIST SP 800-30 to effectively incorporate security risk management. She includes a correlation of the OCTAVE method to NIST SP 800-30 (see Appendix A).

In Section 4.4, Carol Meyers describes how Paradise Valley Community College, a part of the Maricopa Community College District, tailored the OCTAVE approach for security risk management. Carol Myers shares her experience linking information security risk into the college's overall risk management program.

In Section 4.5, Carol Meyers provides a case example of how the OCTAVE method was used in an information technology security risk assessment for the Telescopes in Education Project at Paradise Valley Community College.

## 4.1 Addressing HIPAA-Mandated Risk Assessments with OCTAVE

### Background

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services (HHS) to establish national standards for the security of electronic healthcare information. The final rule [HHS 2003] adopting HIPAA standards for security was published in the Federal Register on February 20, 2003 with two compliance deadlines: (1) April 21, 2005 for all covered entities except small health plans and (2) April 21, 2006 for small health plans.

This final rule specifies a series of administrative, technical, and physical security safeguards for covered entities to use to ensure the confidentiality, integrity, and availability of personally identifiable electronic health information (subsequently referenced as electronic protected health information). The standards are delineated into required or addressable implementation specifications.

The standard §164.308(a)(1) is the security management process. It states that a covered entity must implement policies and procedures to prevent, detect, contain, and correct security violations. Risk analysis and risk management are required implementation specifications for this standard.

**Risk Analysis:** Covered entities must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

**Risk Management:** Covered entities must implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the required HIPAA safeguards.

As part of an early initiative to get a head start in meeting these requirements, the Security Working Integrated Project Team (WIPT), Office of the Assistant Secretary of Defense/Health Affairs (OASD/HA) endorsed OCTAVE as the preferred information security risk assessment approach. The Security WIPT is a subgroup of the HIPAA Overarching Integrated Project Team that has overall responsibility for coordinating the DoD's effort to comply with HIPAA. The Security WIPT is responsible for preparing for compliance with the HIPAA Security Rules. The Defense Health Information Assurance Program (DHIAP) [Collman 2001], a congressionally directed research project administered by the TATRC in Ft. Detrick, Maryland, sponsored the development, testing, and deployment of the OCTAVE method for use in the DoD's medical treatment facilities (MTFs). Because of this sponsorship and OASD/HA endorsement, the DoD used the OCTAVE method to standardize risk assessment at the MTFs while decentralizing the decision-making process during the assessment [Coleman 2003]. The self-directed nature of the OCTAVE approach required

interdisciplinary and inter-hierarchical analysis teams (dubbed Medical Information Security Readiness Teams, or MISRTs) to conduct the analysis for themselves, which resulted in ownership of the process, meaningful results, and relevant and actionable mitigation plans and organizational protection strategies.

### **OCTAVE in the Healthcare Industry**

Under DHIAP and other subsequent programs, the DoD provided OCTAVE method training for MISRTs from over 200 MTFs, firmly establishing the OCTAVE method as a viable and effective methodology for assessing risk in healthcare organizations. Results were documented and presented at major conferences (e.g., the American Telemedicine Association) as a model for (1) using the OCTAVE method to meet the risk assessment requirements for the HIPAA Security Rule and (2) as a foundation for prioritizing mitigation efforts according to organizational needs—a significant step beyond the traditional DoD approach of identifying and mitigating technical vulnerabilities as a separate and isolated activity. Based on this successful report, many healthcare organizations in the private sector followed suit and selected the OCTAVE method to assess information security risk.

As a mature, recognized, and robust methodology, the OCTAVE method has been used to assess information security risk in healthcare organizations that differ in scale, complexity, and geographic location. Comparing the different implementations of OCTAVE tailoring techniques [Alberts 2002] and their results have produced some interesting similarities [Coleman 2004].

First and foremost, the DoD's OCTAVE evaluations were conducted with this objective: execute a risk assessment to meet the HIPAA Security Rule requirements. When results were compared, technical and organizational observations common to several organizations were identified, which suggests that these issues may be prevalent throughout the industry.

### **Implementation Similarities – OCTAVE Phase 1**

Several organizations (ranging in size from small to large) asked general staff members, IT staff members, department managers, and senior managers to fill out Web-based surveys that covered each COP category. Other organizations used workshops and interviews instead, but the Web-based survey presented a number of advantages:

- Individuals at remote sites were included, which increased participation and information security awareness.
- Individuals responded at their convenience, which resulted in more responses and a statistically valid level of participation.

While Web-based surveys have many advantages, the contextual emphasis obtained through facilitated discussions was lost. To counter that, short discussions about current organizational practices and vulnerabilities were included in the senior and operational managers' workshops as appropriate.

Web-based surveys also produced this unexpected benefit: groups that were not uniquely identified in standard OCTAVE method workshops could be discovered. In some MTFs, for example, IT-savvy biomedical staff have sole responsibility for managing biomedical systems independent of IT staff. By comparing survey responses between these two groups with similar IT responsibilities, different perspectives of organizational risk can be identified.

## **Implementation Similarities – OCTAVE Phase 2**

Organizations generally included an in-depth, targeted technical vulnerability assessment focused on critical assets and related components. The scope of the evaluation included stronger consideration of the underlying network architecture when clinical systems were included as critical assets. Many clinical systems (e.g., fetal monitoring and electrocardiogram) are increasingly dependent on the network infrastructure and less frequently deployed as stand-alone systems. In addition, current large-scale systems (e.g., teleradiology), are designed with the network infrastructure as a basic system requirement. To conduct the vulnerability assessment, organizations used scanning tools and manual techniques and also incorporated a physical security review.

For assessments conducted by in-house personnel, the scope was generally focused on systems and infrastructure under direct control of the IT department, which excluded biomedical devices. In cases where the risk assessment was led by external technical consultants, biomedical and other clinical systems were often included as part of the assessment.

Smaller organizations tended to augment their analysis team with technical security experts to assist with this part of the risk assessment. Medium-sized organizations generally conducted this part of the risk assessment in-house with their own security staff. Larger organizations seeking to reach beyond the confines of a traditional IT security assessment used outside experts to conduct the Phase 2 portions of the OCTAVE method. Doing so provides independent validation that IT operational security complies with best practices for security at a technical level. It also enables organizations to investigate technical, physical, and administrative procedures for data handling in systems managed by departments other than IT.

## **Observations From the Organizational View**

In investigating adherence to organizational policies and procedures, most organizations identified clear differences between traditional IT staff and MTF staff responsible for biomedical systems. These differences did not correlate with the organization's size or complexity. In MTFs, basic security measures that control access to biomedical devices containing or accessing patient-sensitive information were often lacking (e.g., shared user IDs for log on). Organizations that surveyed the MTF staff separately identified a significant variance between the IT and MTF staff in understanding and complying with organizational

security policies and practices. Other security challenges identified in the healthcare organizations included

- difficulty with patch management for server farms and internally-managed systems (not vendor-managed systems), which presented numerous problems for the security and IT staff
- difficulty controlling the deployment of service accounts and implementing password changes on accounts that are widely distributed as integral components of health information systems
- difficulty addressing the security of biomedical devices because of concerns about potential vendor warranty issues and challenges in dealing with Food and Drug Administration (FDA) approved systems

## Conclusion

Despite extensive differences in size and complexity among healthcare organizations, a range of common risks and challenges were identified that indicate a consistent level of security risk throughout the industry. The convergence of biomedical devices and IT systems and their growing dependency on the underlying network topology is a prime example. Using a structured industry-recognized methodology that incorporates good standard security practices allows healthcare organizations to identify a sufficient level of security risks to meet HIPAA regulations with effective due diligence. Using a methodology that is sufficiently flexible to include individualized organizational needs allows healthcare organizations to justify their decisions by considering their own unique circumstances and differing abilities to mitigate these risks. OCTAVE is particularly well suited to healthcare organizations. The COP [Alberts 2001b] incorporated into OCTAVE was developed to address the needs of a healthcare organization, and the flexibility of the methodology allows an unlimited number of deployment variations to ensure that the assessment is successful and meaningful.

Organizations' resource limits and the time required to implement effective protection strategies and mitigation plans significantly influenced decisions regarding which risks were ultimately selected for mitigation, deferral, or acceptance. The OCTAVE approach for evaluating risks in terms of organizational impact was critically important and *the* most influential factor considered when prioritizing risks for mitigation. This observation supports the concept of a decentralized decision-making approach to information security in the healthcare industry, which allows organizations to prioritize risks for mitigation according to their own criteria.

## 4.2 Enhancements to OCTAVE by the National Center for Manufacturing Sciences

The National Center for Manufacturing Sciences (NCMS), an organization representing a consortium of manufacturers, has developed extensions to the baseline OCTAVE approach to broaden its applicability to the range of enterprise and value chain vulnerability types important to manufacturing domains. By adding an explicit process modeling step and expanding the definition of a critical asset, vulnerability assessments of high value to the enterprise can be effectively carried out, including

- assessing vulnerabilities of factory floor information technology and systems, including control systems upon which modern manufacturing enterprises depend
- assessing vulnerabilities of classes of enterprise- and mission-critical assets beyond information assets
- assessing the “all-hazards” vulnerability of specific processes with enterprise-critical outcomes, including internal business processes, automated processes, and cross-organizational value chain processes (e.g., supply chains)

Either of the two basic methodologies using the OCTAVE approach originally developed by SEI (the OCTAVE method and OCTAVE-S) can be employed to execute this expanded, process-centric adaptation. The principals and processes of the OCTAVE approach are preserved in the NCMS-extended method, and so are the basic formats (with minor adaptations). NCMS has successfully applied these extensions to assess critical information and physical and process assets for the DoD, manufacturers, and organizations in the utility industry.

### Process-Driven Vulnerability Assessments

NCMS added explicit business process mapping as Phase 0 to initiate the OCTAVE assessment process. This phase provided foundation data for extending the method to various domains of vulnerability. Manufacturers define the value of information assets, and many forms of physical assets, as a byproduct of the business processes and enterprise objectives they support. Thus, organizations that want to assess the vulnerability of their critical assets, both information and physical, can most accurately and comprehensively identify those assets by understanding the highest priority objectives of the enterprise and how those objectives are linked to the organizational business processes.

*Critical processes* typically are core, value-adding processes. If compromised, they would most directly or immediately result in a negative impact on the most important business metrics/objectives or reduce the ability of the enterprise to fulfill its mission. Alternatively, critical processes can support other business processes with high potential of negative business or mission impact should they fail to perform to expected criteria. For example, a subprocess that fails or degrades due to supply chain contamination or data corruption may

cause the loss of an entire production run. By missing a shipment date, an organization may not only lose the order—they may lose an important customer.

*Critical process assets* have one or more of the following qualities:

- They are essential to achieving the minimum output quality and performance criteria in the highest-level process within the scope of the assessment.
- When they are compromised, there is an identifiable potential for major negative impact on the mission, goals, or values of the overall enterprise.
- They are shared among multiple critical processes.

The NCMS process for identifying critical assets through process maps is as follows:

1. Identify and diagram the critical processes to a reasonable level of detail, including descriptions of the inputs and outputs.
2. Precisely identify the process scope for the assessment.
3. Identify and document in-scope process assets.
4. Select a limited set of critical information and physical assets for the critical processes.

### **The Asset View of Processes**

A process model can provide a checklist for identifying assets and a structure for identifying relationships and dependencies so that you can evaluate their criticality. A generic process model starts with an intuitive view of activities bounded by controls, inputs, and outputs. Activities may decompose into subprocesses for effective consideration of larger and complex processes.

The asset view of a process consists of up to seven major components with which assets may be associated and identified:

1. process activities
2. physical and information outputs
3. physical and information inputs
4. output quality and performance criteria
5. input quality and performance criteria
6. tools
7. controls

A generic high-level process model with these seven components is shown in Figure 4. This model is used to document specific processes.

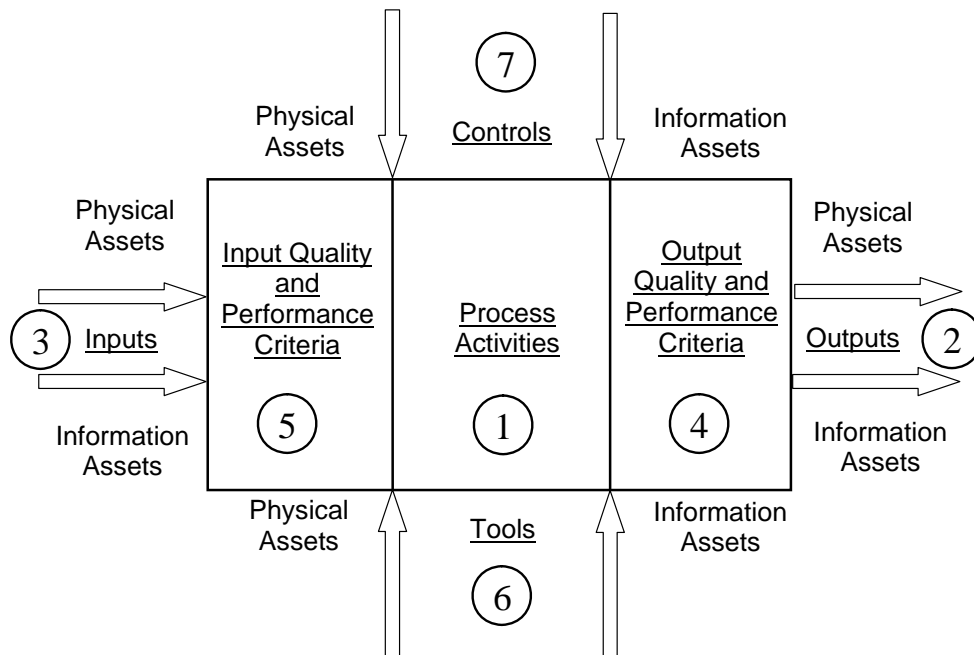


Figure 4: Generic High-Level Process Diagram

The process components *Controls* and *Tools* can be comprised of systems, including—but certainly not limited to—information systems that have both physical and information dimensions. Process assets can be inventoried using these categories, and the most critical assets are candidates for vulnerability and risk assessment. As needed, high-level processes can be hierarchically decomposed into linked subprocesses to expose critical subprocesses, but NCMS experience has shown that consolidating lists of assets from multiple subprocesses at a relatively higher process level is generally sufficient to assure that critical assets are identified.

An example of an asset inventory for a critical manufacturing process is shown in Figure 5.

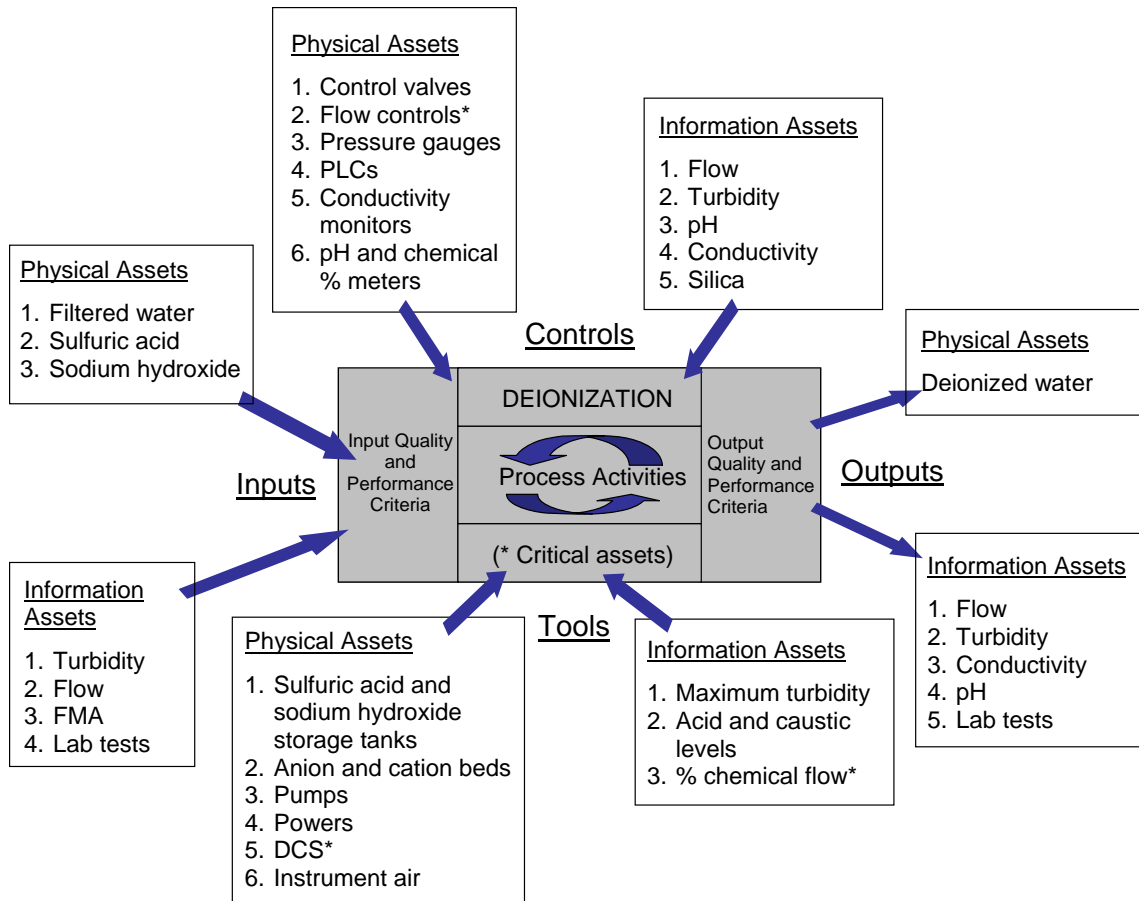


Figure 5: Example Asset Inventory and Critical Asset Identification for a Manufacturing Process

Identifying critical processes, analyzing the asset view of processes, and selecting critical process assets in Phase 1 incorporates the process model information collected in Phase 0. These activities lead in the usual way to the OCTAVE threat tree and recommendations steps, with appropriate adaptations to analysis and presentation formats.

## Conclusion

Through its flexibility in incorporating extensions, the OCTAVE approach has provided NCMS with a robust and repeatable framework to address risk management for DoD and industry customers. In addition, prototypes of a failure analysis method and an NCMS-developed risk management decision process linked within the OCTAVE approach have been successful. The OCTAVE approach is sufficiently robust to support the active management of risks related to asset vulnerabilities of essentially any kind, including physical security, anti-terrorism, and manufacturing process integrity.

## 4.3 Florida Tackles Enterprise Risk Management with OCTAVE and NIST SP 800-30

### Background

Government officials have always had a critical role in protecting their citizens from risks. The risk climate has changed in recent years and handling risk has become more central to the work of government than ever before.

Florida has dealt with information system risks posed by hurricanes, tornadoes, and floods for many years. Information technology plays a major role in state and local government, both fiscally and operationally. The service delivery tools supported by IT have become critical to the mission of all state and local government agencies.

In an era of heightened alerts, state and local governments face extraordinary challenges. They must find and close gaps in the public security network and plan effective responses to critical threats. They need to achieve all this while working under tighter than ever budgets and rapidly changing technologies.

Florida has a long history of technology initiatives and was the first to implement a state Computer Security Incident Response Team (CSIRT) program. The CSIRT program, comprised of teams of employees from each state agency, received critical training from the SEI and CERT/CC at Carnegie Mellon University on responding to computer security incidents. The CSIRT teams were created at the direction of Governor Bush as part of the Florida Infrastructure Protection Center in March 2003.

In a recent study, Florida ranks third in overall IT spending [Workgroup 2005]:

California:	\$3.96 billion
New York:	\$3.77 billion
Florida:	\$2.14 billion
Texas:	\$2.01 billion

Further initiatives passed in the 2004 legislative session prepared Florida to weather incidents caused by computer viruses and cyberterrorism that can have the same, if not greater, impact than a natural disaster. The legislative mandate, Florida Statute 282.318, is known as the *Security of Data and Information Technology Resources Act*. The mandate requires each agency to conduct a risk analysis to identify security threats to data and information technology resources.

Risk refers to the potential of direct or indirect loss due to a failure of people, processes, systems, or external events. This definition acknowledges the uncertainty that underlies much of the work of government. A risk assessment is the first step in creating a risk management program. Identifying operational risks that could potentially prevent an agency from

conducting its mission is the first step to information-protection improvements based on risks to the confidentiality, integrity, and availability of critical information technology assets.

Risk management refers to the ongoing processes involved in identifying, assessing, and judging risks; taking actions to mitigate or anticipate them; and monitoring and reviewing progress. Traditional approaches to information technology risk management are based on compartmentalizing risks and mitigating those risks independently of each other. A paradigm shift is taking place in the business and government communities as many organizations move towards a more holistic model of assessing how risks impact the entire organization. ERM assists in that transition to a higher-level view of information governance and protection. This shift towards an ERM framework can help organizations meet their overall mission, improve service delivery, and save money by using resources more efficiently.

The language of risk management sometimes implies a simpler process than is usually possible in reality. This is particularly the case in state and local government. Government entities deal with more complex operating environments, variables, and conflicting viewpoints than other business fields.

### **Using the OCTAVE Method and NIST SP 800-30 to Assess Risks**

Implementing ERM can be a daunting task, and some states have been reluctant to take on these projects. However, leaders in Florida recognized the value and potential benefits of ERM for their information protection strategies. Benefits of an ERM implementation within government entities include

- preventing problems before they occur
- improving product quality and service delivery
- enabling better use of resources
- promoting teamwork and inter-agency collaboration

State government agencies generally operate autonomously, focused on their individual missions. State and local governments need to assess risks using a methodology that would prioritize the risks according to the subjective needs of the various entities and consider budget, resources, and knowledge. Various methodologies, standards, and guidelines were reviewed, and Florida chose the NIST SP 800-30 [NIST 2002] as a baseline for assessing risk.

Florida selected a third-party vendor to help with the assessments and transfer knowledge to the individual entities. The vendor recommended using portions of the OCTAVE methodology based on the way in which the OCTAVE method aligned with the NIST SP 800-30 standard. The OCTAVE method, combined with the NIST SP 800-30 standard, could be customized to meet the range of needs for the various entities.

As shown in Appendix B, the nine steps of NIST SP 800-30 map directly to segments of the OCTAVE method.

### **Unique Approach to Risk Assessment**

The objectives established for the Florida risk assessments were to define (1) the domain of the information security risks and (2) threats to the IT assets. The traditional self-directed OCTAVE method was tailored to include self-directed and expert-led activities.

The process began with a kick-off presentation for senior managers, operational managers, and business process owners. It introduced the OCTAVE method and how it aligns with NIST SP 800-30 and explained the risk assessment process that would take place over the next few weeks.

The OCTAVE method was tailored to deliver a quality, scope-limited, cost-effective assessment in three to four weeks. In addition, the following items from Process 4 were moved to the beginning of the engagement to more closely align with NIST SP 800-30:

- Create Threat Profiles
- Identify Top 5 Critical Assets
- Refine Associated Security Requirements

To reduce time delays for Process 6, each participating organization identified critical assets and the associated systems *before* the assessment began. That process's technology vulnerability assessment could then be performed in a timely manner. The OCTAVE method was also expanded by the vendor to assess the physical security risks.

Information security policies were reviewed against NIST standards so that gaps could be identified.

NIST SP 800-30 recommends that questionnaires, on-site interviews, existing documentation reviews, and automated scanning tools be used to gather information about the critical assets. Interviews were conducted with key staff members in charge of policy, administration, day-to-day operations, system administration, network management, and facilities management. Interviews were not limited to people directly responsible for the critical assets. People from across the organizations participated, but no formal knowledge elicitation workshops were conducted as recommended in the OCTAVE method. Data was collected on an as-needed basis in a one-on-one interview format.

OCTAVE provides surveys based on the OCTAVE COP. They were used to assess the organization's overall awareness and view of information security.

Risks to intangible assets (e.g., the collective institutional knowledge base) were considered in the analysis. With 64 million baby boomers (over 40 percent of the United States labor

force) eligible to retire by the end of this decade [Morton 2005], state and local governments face significant risk over the next five years.

Phase 2 was tailored based on each organization's capabilities to address technology vulnerabilities within the assets selected in advance for consideration in Process 6. Analysis activities were also tailored to accommodate outsourced partners or third party providers as needed. The NIST SP 800-30 advocates identifying vulnerabilities during system development with specific actions in the systems development, system implementation, and operational phases. The OCTAVE method is structured to identify vulnerabilities of operational systems, which provided a better fit for the project constraints.

Security issues were analyzed in relation to the business issues instead of vice versa (the latter being the more traditional OCTAVE method).

A self-assessment compliance questionnaire was added to the process to satisfy the quantitative and control guidelines in NIST SP 800-30. As a gap analysis and mapping tool, the questionnaire helped highlight areas of security exposure and evaluated the state of readiness for compliance, if required. The questions measured awareness and implementation practices within the security domains of access control, security policy, awareness training, physical security, and incident response procedures, and they were mapped to fundamental elements of information security controls in other regulatory frameworks (e.g., NIST SP 800-53, HIPAA, Sarbanes-Oxley [SOX], and California's 1386 [CA1386] initiative) to expand the level of compliance.

## **Protection Strategy**

Creating a protection strategy to mitigate any identified risks is the second step, after conducting the risk assessment, in an ERM program. Protecting all assets equally is not possible or fiscally sound. After possible threats are detailed and potential impact is assessed, one can decide how to appropriately deal with them. NIST guidelines consider many factors when providing guidelines for implementing controls to mitigate risks.

NIST SP 800-30 assesses the likelihood of a technology vulnerability being exploited, which differs from the OCTAVE approach that considers the likelihood that an asset-threatening event will occur. NIST SP 800-30 guidelines recommend using the probability (high, medium, or low) multiplied by the impact (high, medium, or low) to determine the risk. The OCTAVE method focuses on the risks that would have the greatest negative impact on the mission of the organization. The goal of the risk assessments is to create a strategy to protect the mission of the agency, not just the IT assets.

In NIST SP 800-30, threat sources are listed individually. The NIST SP 800-30 format was used to identify threat sources and then group them based on possible motivations or threat action types. Traditional OCTAVE threat trees were not used to graphically assemble related risks for analysis. By mitigating the most common technology vulnerabilities to protect the critical assets, other assets are protected by association.

The protection strategy developed as a result of the risk assessments could also be used to assess the criticality of system restoration activities after hurricanes or other natural disasters.

## **Lessons Learned**

The biggest lesson learned is that information security and protection of data depends not only on technology but also on each person's awareness of their responsibility to protect critical information assets. Each user has a role in protecting data. Imagine each PC, personal digital assistant (PDA), voice over Internet protocol (VoIP) phone, or other computing device as a front door—there is always the potential for some users to leave the key under the mat.

It is easy to lose focus on the strategic aspects of information security, particularly during Phase 2 when the vulnerabilities were more tactical and the remediation requirements more immediate. Previous security vulnerability analyses focused on technology only. The vulnerability assessments provided a list of technical items to remediate but no overall protection strategy.

The value of the self-assessment compliance questionnaire, which was added to the process to broaden the level of compliance, was unclear. Questionnaire results, without other confirming quantitative measurements, might not accurately reflect actual day-to-day operational practices.

Making a business case for information protection and security—especially in agencies or departments whose primary mission is not related to technology—will take continued effort. IT dependencies are not immediately apparent in agencies and departments whose missions are not traditionally IT-related.

## **Conclusion**

Implementation of an ERM framework, in conjunction with continuous risk management activities using the NIST standards and the OCTAVE method, supports a shift to a risk-smart culture in state and local government. Such a culture supports responsible risk management and builds it into existing governance and organizational structures as well as planning and operational processes. An essential element of a risk-smart culture is to ensure that the workforce has the capacity and tools to innovate while recognizing and respecting the need to be prudent in protecting public interest and maintaining public trust.

Achieving this cultural change will require sustained commitment from state and local government for many years as risk management practices in information security evolve.

As the risk assessment project demonstrated, successful implementation of a continued risk management program requires a combination of visionary leadership, strong commitment, flexibility and innovation, and sufficiently flexible methodologies such as the OCTAVE method.

## 4.4 Paradise Valley Community College Tailored OCTAVE for Security Risk Management

### Background

Paradise Valley Community College (PVCC) is part of the Maricopa Community College District (MCCD) that consists of 10 colleges, two skill centers, and many college satellite centers, including the Arizona state prison. Over 8,000 students are enrolled at PVCC and supported by approximately 200 employees. This translates to roughly 1,600 network hosts.

MCCD has a decentralized administration: each college has a president and a full complement of deans. The district office administration handles core, centralized administrative operations like human resources (HR) and financials. The colleges' missions are diverse: some focus on specific academic disciplines, others on occupational education, and one on distance learning.

Five years ago, MCCD adopted an ERM model that integrates different risk frameworks—based on insurable risks and other types—across the district. The Maricopa Integrated Risk Assessment (MIRA) project embraces ERM because employees can collaboratively identify, assess, and manage future risks and opportunities. In March 2000, the MCCD governing board—with support from the chancellor and the chancellor's Executive Council (CEC)—officially approved MIRA. Later that year, MCCD's risk manager was charged with implementing a multi-year plan.

MCCD's approach to risk management is captured in MIRA's mission statement, which was adopted in 2004: "The Maricopa County Community College District endeavors to be an innovative, flexible higher education institution that encourages risk assessment and management as an integral process for carrying out our mission to promote and enhance student learning and success. It is the responsibility of every employee to identify, assess, and manage risks and opportunities individually, throughout our organization, and to collaboratively strive for continuous quality improvement and the efficient and effective use of our resources." MIRA defined MCCD's posture toward risk as guidance to specifically-focused risk assessments.

### OCTAVE and ERM

MIRA made OCTAVE's flexible methodology a perfect fit for PVCC's information security risk assessment. The OCTAVE method can accommodate all segments of PVCC in identifying assets, threats, and organizational vulnerabilities, and steps can be added quickly to match those items against current security requirements. There are strategies and plans that assist in managing risks and opportunities, protecting and reviewing plans, and developing mitigation strategies for today and the future. The OCTAVE method can be easily tailored to include a hardware and tools inventory covering operating system (OS) and application-level security and security tools.

OCTAVE was narrowed to focus primarily on operational risks and security practices. The MIRA project already garnered top-level buy-in for risk assessment and management. Technology assets would be examined only in relation to good security practices that are part of the OCTAVE COP. Protection decisions would be based on confidentiality, integrity, and availability but directed towards technical infrastructure and staff. Policy and procedural issues identified within or outside of IT would be escalated to the appropriate manager for analysis and potential mitigation based on general business criteria.

OCTAVE for PVCC was distilled into four phases: (1) system infrastructure analysis and documentation, (2) risk and opportunity identification, (3) asset cost analysis, and (4) mitigation strategies and costs. The first two are completed by IT staff, and the latter two are completed by management. The phases are forms driven and consist of check boxes and short answers. The forms are self-explanatory and easy to understand and complete. PVCC relies heavily on them to address the MIRA requirement for a PVCC IT security risk assessment.

## **Conclusion**

PVCC's tailoring of OCTAVE was validated on a course management system that a vendor has just assessed. The OCTAVE and vendor results differed in only one instance: the vendor indicated that information security technical measures were "overbuilt." Participants preferred PVCC's relatively quick and easy information gathering process (via forms and email) over hours of interviews with staff across the organizational unit.

PVCC endeavored to keep the inherent flexibility of the OCTAVE approach present in its model. The end result was to provide a simple vehicle for colleges that would fit easily into their diverse computing environments. This flexibility was validated when another M CCD college implemented PVCC's risk assessment and found it useful.

Feedback suggested that much of the terminology was foreign and sometimes confusing for IT staff. While this is a symptom of first exposure to risk assessment language, it raised the issue of training. For MIRA to succeed, training sessions that cover terminology and basic concepts for risk assessment and the OCTAVE approach should be developed for IT staff and managers.

## **4.5 Case Study: An Information Technology Security Risk Assessment for the Telescopes in Education Project at Paradise Valley Community College**

### **Background**

Science professors have been working on a comprehensive astronomy program through research and various outreach activities. A major initiative within the program is participating in the Telescopes in Education (TIE) project. TIE provides students around the world with the opportunity to remotely control a telescope and charge-coupled device (CCD) camera in a real-time, hands-on, interactive environment. TIE enables students to increase their knowledge of astronomy, astrophysics, and mathematics; improve their computer literacy; and strengthen their critical thinking skills. TIE is sponsored by the National Aeronautics and Space Administration (NASA) and developed through the efforts of numerous volunteers, businesses, and supporting organizations, including the Jet Propulsion Laboratory (JPL) of the California Institute of Technology (Caltech).

The Sky software was purchased last year as the first step required to participate in TIE. To date, a three-server private network connected to a telescope is in place but not in production. The system, which is tentatively called the Paradise Valley Astronomical Connection System (PVACS), was set up using standard business processes but without formal approval from the appropriate PVCC authorities. An astronomy student working under the auspices of a science lab technician designed and deployed the system. A preliminary IT risk assessment of PVACS has been conducted and this evaluation focuses on those results.

### **System Infrastructure Analysis and Documentation**

The astronomy student and system designer provided the documentation. This student is responsible for system support and is available Tuesdays, Thursdays, Saturdays, and Sundays from 10:00 a.m. to 10:00 p.m. All servers, which are detailed in Table 1, are located in the science lab (G144).

Component	Server 1	Server 2	Server 3
Function	Firewall	CCD content	Telescope and CCD camera control
Hardware	<ul style="list-style-type: none"> <li>▪ PII 333</li> <li>▪ PCI 100 Mb/s NICs</li> <li>▪ 128 MG PC100</li> <li>▪ 895 MB Western Digital hard drive</li> <li>▪ Award BIOS rev. 1</li> </ul>	<ul style="list-style-type: none"> <li>▪ Athlon 750</li> <li>▪ 512 MB PC133</li> <li>▪ 10 GB primary hard drive</li> <li>▪ 160 GB netdrive available over LAN, read only</li> <li>▪ BIOS rev. unknown</li> </ul>	<ul style="list-style-type: none"> <li>▪ AthlonXP 3200+</li> <li>▪ 512 MB DDR333</li> <li>▪ 160 GB Seagate ATA hard drive</li> <li>▪ AMI BIOS 1003 for Asus A7N8X deluxe motherboard</li> </ul>
OS	Linux SmoothWall	Windows XP SP 1	Windows XP SP 1
Software/Services	None	<ul style="list-style-type: none"> <li>▪ Apache Web server</li> <li>▪ Symantec Antivirus</li> </ul>	<ul style="list-style-type: none"> <li>▪ The Sky</li> <li>▪ CCDSOFT</li> <li>▪ IAServer, Meade Autostar suite</li> <li>▪ Symantec Antivirus</li> <li>▪ Access database for scheduling</li> </ul>
Ports in Use	None	80	<ul style="list-style-type: none"> <li>▪ 9030</li> <li>▪ 9031</li> <li>▪ 9032</li> </ul>

*Table 1: Server Descriptions for PVACS*

For critical day-to-day functions, PVACS ranks at the bottom of the scale (low) for the college and the astronomy department. Consider that “The telescope control system and content server were made from parts donated which previously were running distributed computing 24 hours/7 days a week and are considered extremely stable.” The system has not yet suffered any repairs or crashes, but they will be documented as they occur. There is no disaster recovery plan because the system was not in production at the time of this evaluation.

Business process risks and security risks identified during the PVCC risk assessment for PVACS are included in Table 2 and Table 3. To comply with the PVCC-tailored OCTAVE forms, mitigating controls and/or processes are provided for each risk.

Rank	Risk	Controls/Processes to Mitigate Risk
1	Personal equipment	Complete and sign donation form (department chair).
2	No contracted support	Employ astronomy student for 12 hours per week for support—funds from science department, work overseen by network administrator.
3	Unsupported, non-production equipment	Submit 2006-2007 budget proposal for two commodity class servers to replace existing development system (departmental responsibility).

*Table 2: PVACS Business Process Risks*

Rank	Risk	Controls/Processes to Mitigate Risk
1	Open port 9030: W32/Bagel worm opens port 9030 as a backdoor	Ports are opened on an exclusive network which does not have access to control of the internal LAN and only limited access to the external one. All ports other than those that are initiated from the LAN side are blocked using the firewall.
2	Windows XP OS	Firewall and anti-virus software are in place.
3	Physical location: servers and switch are in a locked area but open to general traffic. Air temperature, humidity, and circulation are at acceptable levels.	Submit 2006-07 budget proposal for purchasing a locking half rack when purchasing servers (departmental responsibility).

*Table 3: PVACS Security Risks*

The following technology risks are not ranked but require remediation before the system will be approved for full production:

1. There is no formal patch methodology for the Windows XP servers. This will be completed pre-production but will not be initially required for development efforts.
2. There is no system access or account creation procedure in place. Root access will be given to the network administrator for auditing purposes. Strong password methodology using least privilege must be in place. The network administrator will be responsible for assigning additional system administrator accounts based solely on business need.
3. Disaster recover plan must be documented and in place.

## **Asset and Mitigation Strategy Cost Analysis**

If the system's physical assets were sold, they would net approximately \$1,000. Two of the servers were old, decommissioned desktop machines, and one had been refurbished with newer components. The astronomy student owns the network switch and the application software server but is donating the equipment to the college. At this time, asset loss is of little concern to the business operations of the college. PVACS is not instructionally dependent so there is no academic risk to mitigate.

The current configuration is insufficient to meet production security requirements. The Windows XP servers should be combined into one commodity server with larger disk space. One smaller class server, Linux OS, should be purchased to function as a firewall function and host the Apache Web server. Approximate cost is \$10,000. A half-rack with a locking mechanism and a keyboard, video, mouse (KVM) switch will cost \$3,200. Vendors with final quotes that are within the estimated costs will be considered.

## **Conclusion**

This academic year, PVACS should be used strictly as a pilot. The pilot user group should be Physics and Astronomy Club members and other carefully selected physics and astronomy students. System use should not be tied to instruction until all risks are mitigated as described in this document.

---

## 5 About the Contributors

**Johnathan Coleman, CISSP, CISM** is the principal and co-founder of SecurityRiskSolutions, LLC. As deputy director for Information Protection Technology under the congressionally-funded DHIAP, he led the effort in tailoring and delivering OCTAVE training to over 200 DoD Information Security Readiness Teams. As principal of SecurityRiskSolutions, LLC, he is currently assisting several large healthcare organizations in the private sector with their security compliance and information security risk management programs. Johnathan is a visiting scientist at the SEI where he is involved in research, training, and delivery of the OCTAVE method.

**Michael Fancher** leads initiatives by the NCMS in security, assessment, and extended ERM for commercial industry, the DoD, and the public sector. Mike has led the development and application of advanced integrated assessment and risk management frameworks and tools, including adaptations of the OCTAVE method. These frameworks and tools enable enterprise-level leaders and facilities, process, and business unit managers to identify vulnerabilities of many kinds and to consistently manage the range of risks that affect business performance or mission.

**Carol Myers, CISSP**, has worked in IT security for seven years as a designer and information systems security director. She is currently Director of College Technology for Paradise Valley Community College. Her technical background includes software design and development, enterprise systems architecture design and deployment, UNIX administration, database development, and quality assurance. She has presented nationally on open source security tool deployment (EDUCAUSE 2003) and IT security risk assessment methodology and practice (EDUCAUSE/Internet2 Security Professionals 2005 Conference). Carol was program chair for the EDUCAUSE/Internet2 Security Professionals 2005 Conference, vice-chair for the 2004 EDUCAUSE/Internet2 Security Professionals Workshop, 2004-2005 member of the EDUCAUSE/Internet2 Security Task Force. She currently serves on the EDUCAUSE/Internet2 IT Security Risk Assessment Working Group.

**Lisa Young, CISA**, a managing consultant with DynTek Services, Inc., has over 20 years of experience in the information technology and telecommunications industry and has addressed IT governance, information audit and security, and risk management. Lisa is a Visiting Scientist at the SEI teaching the OCTAVE method. In her most recent engagement with DynTek, Lisa was the project manager for 15 of the 24 risk assessments conducted for Florida using the OCTAVE method and NIST SP 800-30 standard. She has extensive experience with regulatory compliance and security operational procedures.



---

## Appendix A    Timeline for OCTAVE in Practice

<b>Date</b>	<b>Action</b>
September 2001	OCTAVE Method v2.0 released for public use
December 2001	OCTAVE Criteria v2.0 published
January 2002	First public offering of OCTAVE method training
March 2002	OCTAVE licensing program initiated
June 2002	<i>Managing Information Security Risks: The OCTAVE Approach</i> is published [Alberts 2002]
September 2002	OCTAVE User's Forum
May 2003	OCTAVE method artifacts available from the CERT Web site
September 2003	OCTAVE-S v0.9 released
February 2004	OCTAVE/NIST SP 800-30 training offered for on-site deliveries
March 2005	OCTAVE licensing program terminated; OCTAVE-S v1.0 released and available from the CERT Web site



---

## Appendix B NIST SP 800-30/OCTAVE Correlation

NIST SP 800-30 is a *standard* that provides guidance on the range of risk management activities for information assets across a system life cycle. Rather than being directive, it provides general guidance on actions that should be accomplished under the umbrella of risk management.

OCTAVE is a *methodology* that focuses specifically on information risk assessment activities. The OCTAVE method incorporates activities for identifying and analyzing information assets, threats, and risk and for forming plans and strategies to mitigate, transfer, or otherwise manage risks to meet NIST SP 800-30 criteria.

Table 4 shows the strong correlation between NIST SP 800-30 steps and the OCTAVE method processes.

<b>NIST SP 800-30 Steps</b>	<b>OCTAVE Phase/Process</b>
Step 1: System Characterization	OCTAVE Phase 1/Processes 1 - 3
Step 2: Threat Identification	OCTAVE Phase 1/Process 4
Step 3: Vulnerability Identification	OCTAVE Phase 2/Process 5 - 6
Step 4: Control Analysis	OCTAVE Phase 3/Processes 7 - 8
Step 5: Likelihood Determination	OCTAVE Phase 3/Process 7
Step 6: Impact Analysis	OCTAVE Phases 1/2/3/Processes 1 - 7
Step 7: Risk Determination	OCTAVE Phase 3/Process 7
Step 8: Control Solutions	OCTAVE Phase 3/Process 8
Step 9: Results Documentation	OCTAVE Phases 1/2/3/Processes 1 - 8

*Table 4: NIST SP 800-30/OCTAVE Method Correlation*





- [Coleman 2003]** Coleman, J. "Execution of a Self-Directed Risk Assessment Methodology to Address HIPAA Data Security Requirements," 224-231. *Proceedings of the SPIE – The International Society for Optical Engineering. Medical Imaging 2003. PACS and Integrated Medical Information Systems: Design and Evaluation*. San Diego, CA, February 18-20, 2003. Bellingham, WA: Society of Photo-Optical Engineering (SPIE), 2003.
- [Coleman 2004]** Coleman, J. "Assessing Information Security Risk in Healthcare Organizations of Different Scale," 125-130. *CARS 2004 - Computer Assisted Radiology and Surgery, 1268 Proceedings of the 18th International Congress and Exhibition*. Chicago, IL, June 23-26, 2004. San Diego, CA: Elsevier, 2004.
- [Collman 2001]** Collman, J. "HIPAA and the Military Health System: Organizing Technological and Organizational Reform in Large Enterprises," 126-131. *Proceedings of SPIE 2001: Medical Imaging, PACS and Integrated Medical Information Systems, Design and Evaluation*. San Diego, CA, February 20-22, 2001. Bellingham, WA: SPIE Press, 2001 (ISBN 0-819-44009-4, TIE ID 11633).
- [Collman 2004]** Collman, J.; Coleman, J.; Sostrom, K.; & Wright, W. "Organizing Safety: The Conditions for Successful Information Assurance Programs." *Journal of Telemedicine and eHealth* 10, 3. (September 2004): 311-320.
- [HHS 2003]** Department of Health and Human Services. "45 CFR Parts 160, 162, and 164. Health Insurance Reform: Security Standards; Final Rule." *Federal Register* 68, 34 (February 2003): 8334 – 8331. <http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf>
- [Morton 2005]** Morton, L.; Foster, L.; & Sedlar, J. *Managing the Mature Workforce*. New York, NY: The Conference Board, 2005. <http://www.conference-board.org>
- [NIST 2002]** National Institute of Standards and Technology, Computer Security Division. *Risk Management Guide for Information Technology Systems*. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf> (2002).

- [Woody 2004]** Woody, Carol. "Applying Security Risk Management to Internet Connectivity in K-12 Schools." PhD thesis, Graduate School of Computer and Information Sciences, Nova Southeastern University, 2004.
- [Workgroup 2005]** Technology Review Workgroup. *Information Technology in the State of Florida: State Agency Chief Information Officers Council*. <http://trw.state.fl.us/downloads/2005TRWFloridaITppt.pdf> (2005).



# REPORT DOCUMENTATION PAGE

Form Approved  
OMB No. 0704-0188

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

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE May 2006	3. REPORT TYPE AND DATES COVERED Final	
4. TITLE AND SUBTITLE Applying OCTAVE: Practitioners Report		5. FUNDING NUMBERS FA8721-05-C-0003	
6. AUTHOR(S) Carol Woody, PhD; Johnathan Coleman; Michael Fancher; Carol Myers; & Lisa Young			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213		8. PERFORMING ORGANIZATION REPORT NUMBER CMU/SEI-2006-TN-010	
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) <p>The CERT Operationally Critical Threat, Asset, and Vulnerability Evaluation<sup>SM</sup> (OCTAVE<sup>®</sup>) method, an approach for managing information security risks, was designed to be sufficiently flexible for organizations to address unique and highly contextual analysis needs through tailoring capabilities. This document describes how OCTAVE has been used and tailored to fit a wide range of organizational risk assessment needs. Guidelines for successful tailoring, built on the reporting practitioners' successes, are provided to help an organization fit the OCTAVE approach to their specific domain and organizational needs. The range of applications demonstrates the flexibility of the OCTAVE approach and its value in addressing security risk management.</p> <p>Readers should already be familiar with the general concepts of the OCTAVE approach.</p>			
14. SUBJECT TERMS security risk management; security risk assessment; OCTAVE; tailoring OCTAVE; HIPAA security risk assessment; NIST 800-30 security risk assessment; Operationally Critical Threat, Asset, and Vulnerability Evaluation		15. NUMBER OF PAGES 50	
16. PRICE CODE			
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL