



Contract No.: DAMD17-01-C-0048
Defense Healthcare Information Assurance Program
(DHIAP)

OCTAVE-Best Practices Comparative Analysis

A Comparison of the
Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM)
Method
and
Commonly Accepted Best Practices for Assessing Information Security Risks
as stated in
The National Institute of Standards and Technology Special Publication 800-30
(NIST SP 800-30)

ATI IPT Technical Report 03-4

June 2003

Prepared for:
U.S. Army Medical Research and Materiel Command
Fort Detrick
Frederick, Maryland 21702-5012

This work was supported by the U.S. Army Medical Research and Materiel Command under Contract No. DAMD 17-01-C-0048. The views, opinions and/or findings contained in this report are those of the authors and should not be construed as an official Department of the Army position, policy, or decision unless so designated by other documentation.



OCTAVE-Best Practices Comparative Analysis

**A Comparison of the
Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM)
Method
and
Commonly Accepted Best Practices for Assessing Information Security Risks
as stated in
The National Institute of Standards and Technology Special Publication 800-30
(NIST SP 800-30)**

ATI IPT Technical Report 03-4
June 2003

Authors:

Scott West, ATI

Archie D. Andrews, ATI

Table of Contents

PREFACE III

1 INTRODUCTION AND BACKGROUND..... 1

1.1 Rationale for Conducting a Comparative Analysis 1

1.2 Documentation Used..... 2

1.3 Overview of OCTAVE 2

1.4 Overview of NIST SP 800-30..... 3

2 COMPARATIVE ANALYSIS..... 7

2.1 Scope..... 7

2.2 Risk Assessment Process 7

2.2.1 Step One: System Characterization 8

2.2.2 Step Two: Threat Identification 10

2.2.3 Step Three: Vulnerability Identification 12

2.2.4 Step Four: Control Analysis..... 15

2.2.5 Step Five: Likelihood Determination..... 15

2.2.6 Step Six: Impact Analysis 16

2.2.7 Step Seven: Risk Determination 17

2.2.8 Step Eight: Control Recommendations..... 17

2.2.9 Step Nine: Results Documentation 18

3 CONCLUSIONS..... 19

4 REFERENCES..... 21

5 GLOSSARY OF TERMS 23

Preface

This report was prepared by the Advanced Technology Institute (ATI) as part of the Defense Healthcare Information Assurance Program (DHIAP). The U.S. Army Medical Research and Materiel Command (MRMC) supports the DHIAP work. The views, opinions, and observations contained in this report are those of the authors and should not be construed as official Department of the Army position, policy, or decision unless so designated by other documentation.

This report is one in a series of reports comparing the OCTAVE Methodology with certain other professional and regulatory requirements that affect Medical Treatment Facilities. Other reports compare OCTAVE with relevant portions of the Security Standards of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Department of Defense Information Technology Certification and Accreditation Process (DITSCAP). The series is designed to provide MEDCOM and MTF management with knowledge of how OCTAVE execution complements and supports regulatory guidance, how the various outputs of these processes might be used to support or substitute for each other, and how to best utilize site staff experienced in one method when conducting another of these methods.

Risk assessment is an important tool in any MTF Commander's or CIO's arsenal of management tools. Proper application of a valid risk assessment not only identifies risks in relation to business, but can also help build a corporate culture of appreciation for risk management throughout the organization. The NIST Special Publication 800-30 provides broad guidance on risk assessment and risk management practices. It defines the standard of commonly accepted best practices. The OCTAVE Methodology is a focused, step-by-step guide to executing a risk assessment on an organization's most critical assets. This report measures the OCTAVE process against the NIST SP 800-30 standards.

The authors have significant experience in technical vulnerability evaluations and security policy and procedure evaluations. They have been intimately involved in teaching the OCTAVE method and assisting MTFs in carrying out OCTAVE assessments. They were assisted in the preparation of this report by extensive discussions with other OCTAVE and risk assessment practitioners and by the many discussions over the course of the DHIAP effort with members of the information assurance team at the Telemedicine and Advanced Technology Research Center: Dr. Jeffrey Collmann, Ms. Kristen Sostrom, and Mr. Willie Wright.

They particularly wish to express their appreciation to Ms. Sarah Hartline for her assistance in the formatting and presentation of this report.

Archie Andrews
Principal Investigator
Defense Health Information Assurance Program

1 Introduction and Background

This analysis compares the information, guidance, and methods used to conduct a risk assessment of a site's critical assets as described in the *Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) Method Implementation Guide* with those of industry best practices and Federal guidelines as reflected in the National Institute of Standards and Technology Special Publication 800-30, "Risk Management Guide for Information Technology Systems" (NIST SP 800-30).

1.1 Rationale for Conducting a Comparative Analysis

The Federal Information Security Management Act of 2002 requires all federal agencies to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency, and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.¹

NIST has issued guidance to help agencies perform self-assessments of their information security programs, conduct risk assessments, and use metrics to determine the adequacy of in-place security controls, policies, and procedures.²

The NIST SP 800-30 has become the measure of a valid risk assessment approach and is commonly referred to as the standard by which risk management programs in the government are measured.³

This document measures the OCTAVE Methodology against the NIST defined standards as found in NIST SP 800-30. If the OCTAVE Methodology supports the value proposition that the NIST standard pre-supposes and provides understandable and useful guidance for accomplishing what the NIST standard advocates, then it should be widely acceptable as a key component of an organization's risk management strategy.

SM Operationally Critical Threat, Asset and Vulnerability EvaluationSM and OCTAVESM are service marks of Carnegie Mellon University. Development of OCTAVE was partially sponsored by the U.S. Army Medical Research and Materiel Command under Contract No. DAMD 17-99-C-9001 and DAMD17-01-C-0048, phases of the Defense Healthcare Information Assurance Program (DHIAP).

¹ *Title III—Federal Information Security Management Act of 2002, E-Government Act of 2002*, P.L. 107-347, December 17, 2002. This act superseded an earlier version of FISMA that was enacted as Title X of the *Homeland Security Act of 2002*.

² National Institute of Standards and Technology, *Security Self-Assessment Guide for Information Technology Systems*, NIST Special Publication 800-26, November 2001; *Risk Management Guide for Information Technology Systems – Recommendations of the National Institute of Standards and Technology*, Special Publication 800-30, January 2002; *Security Metrics Guide for Information Technology Systems*, NIST Draft Special Publication 800-55 (October 2002).

³ U.S. General Accounting Office, *Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, D.C.: January 2003).

1.2 Documentation Used

The documents describing the OCTAVE Method and a standard for information risk assessment best practices used in this comparative analysis are:

- The OCTAVE Method Implementation Guide, Version 2.0, Volumes 1-18;
- The OCTAVE Criteria, Version 2.0; and
- National Institute of Standards and Technology Special Publication 800-30, “Risk Management Guide for Information Technology Systems” (NIST SP 800-30), 2001.

1.3 Overview of OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Methodology provides a means for an organization to understand and address organizational and technical information security risks. The OCTAVE Methodology has been developed by the Software Engineering Institute as a risk assessment methodology suitable for use by public and private organizations under the sponsorship of the Department of Defense. MHS has selected OCTAVE as the preferred approach for DoD medical facilities to use in preparing to comply with various HIPAA requirements.

The OCTAVE Method guides a site through a qualitative information risk analysis methodology designed to identify:

- Information assets critical to the organization or site;
- Threats to those critical information assets;
- Vulnerabilities associated with those information assets; and
- Current levels of risk in regard to the security of those critical information assets.

The OCTAVE methodology also helps the site to better organize the results of their information risk assessment in order that they may develop or refine proper, effective, and pertinent security protection strategies and risk mitigation plans tailored for that site’s security requirements.

The OCTAVE methodology includes activities conducted before the assessment and eight main process steps executed in three phases.

- In **Startup**, site staff perform preparation activities that include obtaining senior management sponsorship for conducting the OCTAVE, selecting site-knowledgeable individuals from operational areas and IT who will serve as the evaluation’s “analysis team” (the core group responsible for leading and executing OCTAVE activities), and providing appropriate types of OCTAVE-related training to the analysis team and other site participants.
- In **Phase 1**, the analysis team conducts a workshop with senior management to identify the organization’s critical information assets and document threats to the assets, security requirements for the assets, current protection strategy practices, and current organizational vulnerabilities (i.e., weaknesses in organizational policies and practice). The team then works with senior management to select the operational areas to be included in the scope of the OCTAVE evaluation.

The team conducts a workshop that is nearly identical to the senior management workshop with the managers of the selected operational areas (i.e., the “operational managers”) to

capture their perspectives regarding the same subjects. The same workshop is conducted with staff-level individuals from the same operational areas and a similar (but more technically oriented) workshop is conducted with members of the IT staff. The analysis team uses the site staff input to determine the mission-critical assets that will be examined and compile the information collected for these assets into a set of Threat Profiles which establish the basis for the rest of the OCTAVE evaluation.

- In **Phase 2**, the analysis team works closely with the IT staff (or external resources if necessary) to identify “systems of interest”—those systems that are closely related to each important asset—and the infrastructure components related to them. They use software tools to conduct a vulnerability analysis of technical components that are key to the site’s processing of the critical assets, review the identified vulnerabilities, and prepare a summary of results.
- In **Phase 3**, the analysis team completes the risk analysis by consolidating information generated from the organizational evaluation of Phase 1 and the information infrastructure assessment of Phase 2. They complete development of organization-specific risk evaluation criteria to determine what would constitute a high, medium, or low impact on the organization. The team then updates the threat/risk profile for each asset with impact descriptions and applies the risk evaluation criteria to document whether each risk (i.e., threat/impact) would have a high, medium, or low impact.

Using the information created in Phase 1 when senior/operational management and staff compared site security practices to the Catalog of Practices combined with the results of the preceding risk assessment, the analysis team drafts a Protection Strategy that will preserve the good practices present in the organization while also addressing the organizational vulnerabilities identified during OCTAVE execution. They then develop Risk Mitigation Plans for the critical assets, and they develop a list of near-term actions identified as necessary during development of the longer-range strategy and plan. The phase concludes with the analysis team meeting with site senior management to review the site risk information gathered throughout the process and review/adjust the draft Organization Protection Strategy, Risk Mitigation Plans, and Action List. This activity is designed to capture senior management commitment to the OCTAVE results, have them apply their knowledge to tailoring the results to fit even more closely with the mission and goals of the organization, finalize content of the Protection Strategy/Risk Mitigation Plans/Action List, and arrange to initiate actions to implement the OCTAVE-identified improvements to site information protection capabilities.

1.4 Overview of NIST SP 800-30

National Institute of Standards and Technology Special Publication 800-30 is a set of guidelines for managing information security risk written for use by Federal and non-governmental organizations. The guidelines are written to provide a foundation for the development of an effective information risk management program based on the protection of information technology assets by addressing technical and non-technical functions that may influence information security risks.

OCTAVE-Best Practices Comparative Analysis

NIST SP 800-30 is written to give the reader a better understanding of and appreciation for risk management, as well as to provide a demonstrable means of managing risk to their information assets. NIST SP 800-30 provides the reader with guidelines and information about the crucial elements of information risk management to include information risk assessment, risk mitigation, and continual evaluation and assessment. NIST provides an overview and guidance in relation to the following elements of information risk management:

- *Information Risk management in the software development life cycle (SDLC).* NIST SP 800-30 includes guidance on how and when to include risk management in the SDLC. NIST encourages the reader to look at the SDLC as a five-phase process and directs the reader as to what risk activities are appropriate to each of those phases.
- *Nine-step methodology for conducting information risk assessment.* The methodology for assessing information risks described in NIST SP 800-30 is intended to provide a systematic approach to risk assessment by guiding the reader through a series of steps, with guidance on inputs to and outputs from the processes described in each step and how each step in turn leads to and supports subsequent process steps. The NIST view of a risk assessment process includes the following nine steps:
 - Step One -- System Characterization. During Step One of the NIST risk assessment process, the function, criticality, and sensitivity of those assets included in the assessment boundary are defined through a set of information gathering techniques.
 - Step Two – Threat Identification. Threat sources are identified and grouped with possible motivations and threat actions.
 - Step Three – Vulnerability Identification. A list of technical and non-technical vulnerabilities associated with IT systems that could be exploited by potential threat-sources is developed during Step Three.
 - Step Four – Control Analysis. The purpose of control analysis is to examine the effectiveness of the current controls that have been implemented, or are planned for implementation, to minimize or eliminate the likelihood of a threat exploiting vulnerability.
 - Step Five – Likelihood Determination. The probability that a threat source may exploit a potential vulnerability in an information asset is determined during Step Five.
 - Step Six – Impact Analysis. The adverse impact resulting from a successful exploitation of a vulnerability by a threat source is determined.
 - Step Seven – Risk Determination. The purpose of Step Seven is to determine probable levels of risk to the site information assets.
 - Step Eight – Control Recommendations. Controls that mitigate or eliminate information risks identified in earlier steps of the risk assessment are examined.
 - Step Nine – Results Documentation. All results of the information risk assessment are documented.

- *Risk mitigation process.* NIST SP 800-30 provides guidelines and information for prioritizing, evaluating, and implementing risk-reducing controls from the information risk assessment.
- *Good practice for ongoing risk management.* Good practice and the need for ongoing information risk evaluation and assessment are discussed in the final section of NIST SP 800-30.

The NIST special publication also provides the following tools and appendices designed to support the guidelines presented in NIST SP 800-30, as well as assist the reader in the information risk management process:

- Tools and formulas for determining risk levels to information assets;
- The advantages and disadvantages of performing qualitative and quantitative information risk assessments;
- A list of sample interview questions; and
- A sample information risk assessment report outline.

2 Comparative Analysis

This report will compare the OCTAVE Methodology to the recommended best practices outlined in NIST SP 800-30. The comparative analysis is based on the nine-step risk assessment process recommended in NIST SP 800-30, and maps the process steps to equivalent processes found in the OCTAVE Methodology Implementation Guidance.

The nature of the comparison requires the authors to compare not only at the high-level, but also at the detailed implementation level. As in any comparison, it is important to set the parameters of the two items being examined to ensure that only like qualities are compared and contrasted. The largest challenge has been to ensure that the semantic meanings attached to the details within each of the recommended processes are matched for a reasonable comparison.

2.1 Scope

NIST SP 800-30 provides guidance on the range of risk management activities for information assets across a system life cycle. Rather than being directive in nature, this document provides general guidance on actions that should be accomplished under the umbrella of risk management. Besides the nine-step process it describes for risk assessment, it also includes guidance on other aspects of information risk management to include:

- Managing risk in the software development life cycle;
- Information risk mitigation options and strategy;
- Approaches for implementing security controls;
- Guidance on Cost-Benefit analysis; and
- Identifying and managing residual risk to information assets.

In contrast, OCTAVE's content focuses specifically on the activities pertinent to conducting an information risk assessment. OCTAVE provides a deeper analysis of information risk assessment than NIST SP 800-30. OCTAVE explains in detail methods for identifying and analyzing information assets, threats, and risk, and formulating plans and strategies to mitigate, transfer, or otherwise manage risks.

2.2 Risk Assessment Process

NIST SP 800-30 describes a nine-step risk assessment as part of risk management. OCTAVE assesses risk to information assets through a three-phased methodology consisting of eight steps, referred to as "processes" in the OCTAVE documentation. Pre- and post-assessment activities are not included as part of OCTAVE's eight steps, but are included in the OCTAVE Method Implementation Guides, and are mentioned in appropriate areas of the comparative analysis.

Since both methods are used to assess risk to information assets, they are similar in general concept. Differences in each method's approach to information risk assessment are based on specific risk assessment tasks and expected outcomes. This section compares the methodical approach of OCTAVE to that stated in the nine steps of NIST SP 800-30.

It should be noted that NIST SP 800-30 and OCTAVE use different phrasing to describe a similar series of events. Risk assessment activities as described in NIST SP 800-30 are conducted in a series of "Steps." OCTAVE has a similar temporal timeline of execution, but the

OCTAVE-Best Practices Comparative Analysis

steps are referred to as “Processes.” Therefore, the Processes of OCTAVE will be compared to the Steps of NIST SP 800-30.

2.2.1 Step One: System Characterization

During Step One of the NIST risk assessment process, the function, criticality, and sensitivity of those assets included in the assessment boundary are defined through a set of information gathering techniques. The preliminary assessment activities of OCTAVE, as well as OCTAVE Processes One through Three, use similar techniques to gather similar information.

The following properties of NIST SP 800-30 are used as a basis for comparison of OCTAVE with best practices:

- Asset Selection and Assessment Boundary;
- Information Inputs; and
- Information-Gathering Techniques.

2.2.1.1 Asset Selection and Assessment Boundary.

At the center of both the NIST and OCTAVE risk assessments is an information asset. Both the NIST and the OCTAVE risk assessment methods are concerned with bounding the area of consideration so that the assessment is executable and meaningful to the organization. The NIST process guidance recommends defining the scope of the effort as the first step. The risk assessment boundaries are IT system-centric and concentrate on identifying the boundaries of the information system to establish the scope of the risk assessment. Thus, the risk assessment team is given the task of either taking on the entire IT infrastructure as the area under investigation or partitioning the IT systems based on functional requirements, users, or the point in the system life cycle (e.g., design, under development, or operational). The NIST guidance alludes to taking a practical approach, doing what makes sense for the particular circumstances or life cycle of the systems under investigation, but not necessarily focused on any one information asset or system.

The OCTAVE Methodology takes a slightly different approach. The OCTAVE principle is to spend effort on identifying those information resources that are most critical to the continuation of the organization’s core missions; thus, OCTAVE is focused on operational systems that have an immediate effect on the organization.⁴ The rationale for this partitioning of effort is to maximize return on investment by focusing risk management activities on those system resources that will have the most potential impact on the organization’s mission. The underlying philosophy is that any improvements impacting the most critical assets will have a beneficial side effect on all of the organization’s assets and operational procedures. In addition, the organizations’ discussion and group consensus on what their critical assets are and how those assets contribute to the organization’s mission not only provide a good means of bounding the effort required to do a risk assessment, but it also adds weight and validity to performing the risk assessment.

⁴ The authors are aware of a number of occasions when OCTAVE was used as a risk assessment methodology in the design and development stages in order to build security considerations into the design/development processes with success.

The OCTAVE guidance recognizes that this selective approach will not include all information assets in the risk assessment. The guidance does recommend periodic risk assessments conducted to address other information assets that may have been overlooked in the first OCTAVE, or whose criticality has changed. OCTAVE Methodology provides a rational means of applying meaningful limitations to the scope of an information resource risk assessment especially when the IT systems under investigation are operational systems.

2.2.1.2 Recommended Documentation to Aid the Risk Assessment Process.

The documents shown in Table 1 are representative of the documentation recommended for use in both NIST SP 800-30 and OCTAVE. Like NIST SP 800-30, OCTAVE encourages the site to gather as much pertinent existing information about site assets as possible to better understand site assets and facilitate the risk assessment process.

Table 1. Recommended Documentation

| NIST SP 800-30 | OCTAVE |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • Hardware • Software • System Interfaces • Data and information • Persons who support the IT system • System mission • System and data criticality • System and data sensitivity • Asset functional requirements • System Users • System security policies, protection requirements, laws, industry practices • System security architecture • Network topology • Information storage protection • Information flow • Technical security controls • Managerial security controls • Operational security controls • Physical security environment • Documented and undocumented procedures and practices | <ul style="list-style-type: none"> • Organization chart • List of computing equipment • Software Inventory • Network diagram • Security policy documentation • Security procedure documentation • Architecture documentation • Security training materials • Router configuration tables • Logs and audit data • Tool configurations • Security newsletters • List of available vulnerability evaluation tools, checklists, and scripts for operating systems, applications, and physical security |

2.2.1.3 Information Gathering Techniques.

NIST SP 800-30 recommends that *questionnaires, on-site interviews, existing documentation review, and automated scanning tools* be used to gather information about the information assets.

These same information-gathering techniques are incorporated as an integral part of the OCTAVE evaluation with specific guidance. Each technique is explained in the OCTAVE Method Implementation Guide:

- *Questionnaires.* OCTAVE provides detailed questionnaires based on the OCTAVE “Catalog of Practices.”
- *On Site Interviews.* The workshops and guidance of the first three processes of OCTAVE describe information-gathering techniques designed to identify organizational areas of concern, security requirements, current protection strategies, and organizational vulnerabilities. These techniques include detailed question and answer interaction with OCTAVE participants.
- *Existing Documentation Review.* Guidance from Volume Two of the OCTAVE Method Implementation Guide recommends gathering all available relevant documentation that may be useful to the assessment prior to OCTAVE Process One.
- *Automated Scanning Tools.* Basic guidance on the use of automated scanning tools is provided in the OCTAVE Method Implementation Guide, and encouraged during Phase Two (Processes Five and Six) of OCTAVE.

2.2.2 Step Two: Threat Identification

Step Two of the NIST risk assessment process focuses on identifying threat sources and grouping them together on the basis of possible motivations and threat actions. The two main concepts of Step Two of the NIST risk assessment process are threat-source categories and techniques for identifying and documenting threats. In OCTAVE Process Four, threat-sources, motivators, and possible outcomes are identified for each critical asset.

2.2.2.1 Threat Source Categories

In NIST SP 800-30, threat sources are listed individually, and may fall into one of the following categories:

- Human threats, such as unintentional modification, deliberate modification, authorized and unauthorized access
- Environmental threats, such as power failures, bursting water pipes, chemical spills, etc.
- Natural threats, such as floods, earthquakes, tornadoes, hurricanes, etc.

Though OCTAVE does not require that specific threats be listed, general threats are grouped into categories based on their sources. These categories are very similar to the threat source categories explained in NIST SP 800-30, and can be tailored by the site to include specific threat sources. OCTAVE threat-source categories are shown below:

- Human actors using network access
- Human actors using physical access

- System problems, such as hardware and software defects, viruses, malicious code, unavailability of related systems
- Other problems out of the organization’s control, such as natural disasters, unavailability of systems maintained by other organizations, broken water pipes, global telecommunication outages.

2.2.2.2 Techniques for Identifying and Documenting Threats

By using a tabular approach, NIST SP 800-30 identifies unique threat sources from one of three threat-source categories and associates the threat source with motivation and a threat action. The threat-source, motivation, and threat actions table is regarded as the threat statement, and is the output of Step Two. The information in the threat statement is later used in Step 3 to identify vulnerabilities.

An example of a threat statement may look similar to the one shown in Table 2.

Table 2. NIST SP 800-30 Threat Statement for Computer Criminals

| Threat Source | Motivation | Threat Actions |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Computer Criminal | <ul style="list-style-type: none">• Destruction of Information• Illegal information disclosure• Monetary gain• Unauthorized data alteration | <ul style="list-style-type: none">• Computer Crime• Fraudulent Act• Information bribery• Spoofing• System Intrusion |

OCTAVE uses methods similar to those suggested by NIST for identifying threat sources. While NIST describes the use of tables to help a site identify potential threats, OCTAVE provides empty threat trees for each threat-source category, as well as example threat trees in the OCTAVE documentation. The OCTAVE threat trees allow the analysis team to trace each threat-source’s access point, motivation, and the potential outcome of the threat in general terms such as “disclosure,” “modification,” “loss,” “destruction,” and “interruption.” This increases the analysis team’s ability to understand and duplicate the threat identification process recommended as best practice for information risk assessments.

An example of an OCTAVE threat tree is shown in Figure 1.

Figure 1. OCTAVE Threat Tree, “Human Actors Using Network Access”
Human Actors Using Network Access

| ASSET | ACCESS | ACTOR | MOTIVE | OUTCOME | IMPACT |
|-------|---------|---------|------------|-------------------|--------|
| | | | | disclosure | |
| | | | accidental | modification | |
| | | | | loss, destruction | |
| | | | | interruption | |
| | | inside | | | |
| | | | deliberate | disclosure | |
| | | | | modification | |
| | | | | loss, destruction | |
| | | | | interruption | |
| | network | | | | |
| | | | | disclosure | |
| | | | accidental | modification | |
| | | | | loss, destruction | |
| | | | | interruption | |
| | | outside | | | |
| | | | deliberate | disclosure | |
| | | | | modification | |
| | | | | loss, destruction | |
| | | | | interruption | |

2.2.3 Step Three: Vulnerability Identification

Vulnerability Identification is designed to develop a list of technical and non-technical vulnerabilities associated with IT systems that could be exploited by potential threat sources. During Step Three, the NIST guidance describes the vulnerability identification process as part of the software development life cycle, as well as a means of identifying vulnerabilities in operational systems.

2.2.3.1 Vulnerability Identification During the Software Development Life Cycle

NIST recommends that vulnerability identification take place during the system design phase, system implementation phase, and while the system is operational. During the system design phase, the focus of vulnerability identification should be on organizational security policy, planned security procedures, system requirements definitions, and vendor or developer security product analyses. In the system implementation phase, the focus of vulnerability identification should include specific information such as planned security features described in the security design documentation and the results of system test and evaluation. For operational systems,

vulnerability identification should include an analysis of the technical and procedural IT system security features and the security controls used to protect the system.

The OCTAVE Methodology is primarily focused on operational systems, but it may be tailored to consider vulnerability identification in the software development life cycle. Though OCTAVE does recognize that poor management, administration, and staff practices may introduce vulnerabilities to information technology assets, the OCTAVE documentation does not provide specific guidance for identifying technological system vulnerabilities based on that system's place in the software development lifecycle. While such methods are not explicitly part of the OCTAVE documentation, the OCTAVE vulnerability identification process does include flexibility to adapt OCTAVE's methodology to specific phases of the software development life cycle based on high-level best practice guidance provided in NIST SP 800-30.

2.2.3.2 Methods Used in Vulnerability Identification

NIST suggests that three techniques be used to identify and learn about potential vulnerabilities affecting technical assets. They are:

- Vulnerability Sources;
- System Security Testing; and
- System Security Requirements Checklists.

Vulnerability sources. Vulnerability sources are technical and non-technical vulnerabilities associated with an IT system's processing environment. They include information repositories that contain detailed descriptions about well-known vulnerabilities associated with deployed system software, hardware, and configuration, as well as practical matters such as water sprinklers providing fire suppression in a data center. Vulnerability sources may be found in industry periodicals or websites, past risk assessment reports, system audit reports, system logs, vulnerability lists, and vendor security advisories. The intent is to build a correlation between potential exposures and known vulnerabilities in order to plan remediation.

OCTAVE takes a more pragmatic approach to the identification of potential vulnerabilities, focusing on those portions of the infrastructure that are key components for the critical assets. Thus, if the critical systems are Unix-based, for instance, then the focus of the search for potential vulnerabilities specifies Unix vulnerabilities. This practical, focused approach fits in well with the NIST recommended practices.

System Security Testing. NIST recommends the following system testing methods to identify vulnerability:

- Use of automated vulnerability scanners;
- Security test and evaluation (ST&E); and
- And system and network penetration tests.

NIST SP 800-30 provides high-level guidance as to why these techniques are used, but refers the reader to NIST SP 800-42, "Network Security Testing Overview," for complete guidelines describing a methodology for network system testing and using automated security-testing tools.

OCTAVE-Best Practices Comparative Analysis

OCTAVE provides managerial guidance and advice in identifying technical vulnerabilities through security testing. Technical security testing of the information assets is left to skilled technical personnel, and is not covered in complete, low-level detail, as it is in NIST SP 800-42. Instead, enough information is given to the OCTAVE analysis team so they understand the *management* of the security testing effort. It leaves the technical details of the system security testing to the technical experts, but gives sufficient guidance so that the analysis team should be able to ask the right questions. The OCTAVE documentation adds to the managerial understanding of the security testing effort by also providing information about the different types of vulnerability tools, their capabilities, and their limitations. The OCTAVE approach gives the analysis team sufficient understanding to appreciate the value of ongoing system security testing and to assess whether current system security testing is adequate.

System Security Requirements Checklists. The NIST SP 800-30 provides general areas of concern in order for the government agency to formulate a system security requirements checklist. The intent of the checklist is to ascertain whether existing or planned security controls are meeting or will meet the security requirements for the system. Such a checklist, when created, should contain basic security standards that can be used to evaluate and identify information security vulnerabilities in personnel, hardware, software, and information assets, as well as vulnerabilities in non-automated procedures, processes, and information transfers associated with IT systems.

NIST also recommends the use of the questionnaire available in SP 800-26, “Security Self-Assessment Guide for Information Technology Systems.” The referenced questionnaire is based on requirements found in statute, policy, and guidance on security and privacy.

The OCTAVE Methodology is not focused on a standing set of regulatory requirements and policy guidance. Rather, the security requirements assessed and evaluated in OCTAVE are more generic and refer to the universal requirement that the availability, confidentiality, and integrity of an information asset must be protected. Security requirements in OCTAVE do not refer to a specific set of documented requirements, such as the Privacy Act, HIPAA, or NIST standards, but instead refer to the organization’s view of what aspect of security is required in terms of protecting the availability, confidentiality, and/or integrity of the information in that asset. For instance, an asset, such as a router or a switch, may be essential for transferring information across a critical network. Without this router or switch, the exchange of critical information may be severely degraded, so the site requires that the network path provided by this router or switch always be available. Therefore, availability is the security requirement for this asset.⁵

In order to ascertain whether existing or planned security controls are meeting the security requirement for a particular component of a critical system, as well as to identify other organizational vulnerabilities, OCTAVE recommends the use of organizational surveys based on the OCTAVE “Catalog of Practices.” The “Catalog of Practices” is based on a collection of tested and proven strategic and operational security practices. Like OCTAVE, the “Catalog of Practices” is not specific to any domain, organization, or set of regulations and may be tailored to

⁵ Security Requirements as defined in Volume 14 of the OCTAVE Method Implementation Guide: Security requirements outline the qualities of information assets that are important to an organization. Security requirements reflect a requirement for the confidentiality, integrity, and availability of a critical asset to be protected.

incorporate specific language, requirements, regulations, and standards of the organization conducting the OCTAVE. As such, the surveys based on the “Catalog of Practices” may also incorporate guidance as provided in NIST SP 800-26, and may be easily adapted for use as checklists. The intention of the NIST recommended practice of identifying and considering security requirements associated with a particular system(s) is met by the OCTAVE incorporation of the “Catalog of Practices” and the emphasis in OCTAVE of assessing the basic attributes of confidentiality, integrity, and availability.

2.2.4 Step Four: Control Analysis

The purpose of control analysis is to examine the effectiveness of the current controls that have been implemented, or are planned for implementation, to minimize or eliminate the likelihood of a threat exploiting a vulnerability. NIST categorizes security controls as technical or non-technical. Technical controls protect computer hardware, software, and firmware; non-technical controls protect management and operational procedures. Non-technical controls are categorized as security policies, operational procedures, personnel, physical, and environmental security. NIST also recommends a checklist approach to evaluate these controls.

Like NIST SP 800-30, OCTAVE also requires that current, implemented and planned controls be examined. Before new controls are determined in the last stages of OCTAVE, current controls are reviewed and refined as the analysis team compiles and reviews the results of the OCTAVE surveys. The OCTAVE surveys based on the “Catalog of Practices” cover technical and non-technical control implementations, and are the main mechanism used by the analysis team to determine effectiveness of current controls.

2.2.5 Step Five: Likelihood Determination

NIST devotes a step for determining the probability that a threat source may exploit a potential vulnerability in an information asset. NIST advises that the assessment team categorize the likelihood of such an event as either high, medium, or low based on an examination of the prior steps’ outputs. The outputs of the first four steps should give the assessing team enough material to consider the threat-source motivation and capability, nature of the vulnerability, and existence and effectiveness of current controls.

The use of likelihood determination in the information security risk assessment is an issue on which NIST and OCTAVE differ philosophically in how they determine risk. Likelihood of occurrence is not considered in the current version of OCTAVE. Rather, the designers of the OCTAVE method took the approach that unforeseeable changes in the information security environment make predicting the probability that a particular information system may be exploited too imprecise to be of real use in an information security risk assessment, and that a vulnerability, no matter how arcane in the current environment, may be a prime candidate for exploitation once discovered.⁶

⁶ Alberts, Christopher J. and Audrey Dorofee. OCTAVE Method Implementation Guide, Version 2, Volume 9, pg. G7-9

2.2.6 Step Six: Impact Analysis

During the impact analysis, the adverse impact resulting from a successful exploitation of a vulnerability by a threat source is determined. The major activities of this step as recommended by the NIST guidance are to:

- Gather pertinent documentation about the asset's mission, criticality, and data sensitivity;
- Create this information if it is not available;
- Create quantitative or qualitative values for defining impacts; and
- Define the impact of an exploited vulnerability in terms of a loss of information integrity, availability, or confidentiality.

OCTAVE guides the analysis team to use high, medium, and low criteria to describe the impact that an exploitation of security vulnerability has on the organization under the assumption that such a security breach occurs. This approach guides the site to base priorities for risk mitigation on the potential mission impact.

2.2.6.1 *Gather or Create Documentation*

Using the guidance in NIST SP 800-30, documentation is gathered but not used early in the evaluation. If no documentation is available, it is created in Step Six of the NIST risk assessment. OCTAVE also gathers documentation before the assessment, but begins to create or use such documentation in the initial processes of the evaluation. Documentation that describes the critical assets and outlines their security requirements as defined in OCTAVE is created in asset profiles during the first four processes of OCTAVE.[†] Documentation that is created as a result of the workshops in OCTAVE Processes 1-7, as well as the surveys, is compiled and reviewed prior to the creation of new mitigation plans and security strategies in OCTAVE Process Eight (a).

2.2.6.2 *Quantitative versus Qualitative Values*

NIST SP 800-30 explains the advantages and disadvantages of conducting quantitative and qualitative risk assessments for consideration, but provides no guidance as to which is the preferred practice; the decision about quantitative versus qualitative impact analysis is situational dependent.

Since OCTAVE does not consider probability, a necessary element in factoring quantitative values, only qualitative techniques to assessing risk are explained. OCTAVE does encourage tailoring the assessment to meet the needs of the site, and, in OCTAVE Process Seven, also notes that monetary values may be associated with high, medium, and low impact categories as a means of stressing urgency or priority for management consideration.

[†] Security Requirements as defined in Volume 14 of the OCTAVE Method Implementation Guide: Security requirements outline the qualities of information assets that are important to an organization. Security requirements reflect a requirement for the confidentiality, integrity, and availability of a critical asset to be protected.

2.2.6.3 Impact Terminology

Impacts as described in NIST SP 800-30 are categorized as high, medium, or low based on predefined impacts or consequences of an exploited vulnerability.

OCTAVE pushes the organization to define impacts itself, and eventually prioritize risk mitigation and protection strategies. OCTAVE uses the security requirements definition to determine whether the confidentiality, integrity, or availability of an asset is most important to the site mission. The outcomes of the threat trees are then stated in terms of “disclosure” (the loss of confidentiality), “modification” (loss of integrity), “loss/destruction” (loss of integrity/availability), and “interruption” (loss of availability). Therefore, “outcomes” in OCTAVE are analogous to what NIST refers to as “impacts.”

In OCTAVE, the impacts are defined as a threat’s effect on the organization, and the net effect within areas that have tangible corollaries to the mission or business health of the organization are assessed. The analysis team is lead through the thought process of assessing the impact on the organization in such areas as reputation/customer confidence, life/health of customers, fines/legal penalties, and financial.

2.2.7 Step Seven: Risk Determination

Risk determination in NIST SP 800-30 is to assess the levels of risk to the site assets. Likelihood is a part of the risk determination process described by NIST, as well as the results of the impact analysis from step five, and analysis of the adequacy of planned or existing security controls. This step considers the probability of exploitation of a vulnerability.

OCTAVE Methodology takes a different approach. Rather than considering the product of probability (high, medium, low) times impact to the organization (high, medium, low) as NIST 800-30 recommends, OCTAVE directs the analysis team to focus on impact to the organization’s mission and make that impact the prime consideration in developing risk management mitigation plans and strategies.

2.2.8 Step Eight: Control Recommendations

Controls that mitigate or eliminate risks identified during execution of the steps recommended by NIST SP 800-30 are examined in Step Eight, Control Recommendations. NIST guidelines include the consideration of several factors before recommending controls and alternative solutions to minimize risks. These controls include the effectiveness of the recommended options, legislation, regulation, organizational policy, operational impact, safety, and reliability of the risk control mechanisms. NIST encourages the site to conduct a cost-benefit analysis to determine if the recommended controls are worth the cost of implementation, as well as to consider the operational impact and feasibility of introducing certain mitigating controls.

Control recommendation occurs as the culmination of the OCTAVE evaluation. Based on the compiled results of the preceding OCTAVE processes, the analysis team develops a set of recommended protection strategies, mitigation plans, and a list of near-term action items for the organization. These control recommendations are then presented to the senior managers for their approval and resource commitment. The senior managers make final adjustments to the recommended controls and define the next steps required to implement the controls.

2.2.9 Step Nine: Results Documentation

All results of the risk assessment are documented in step nine of NIST SP 800-30. The risk assessment report is used as a management report to help senior managers make decisions about policy, procedural, budget, and system operational and management changes.

Each process of OCTAVE provides a means of documenting the process workshop results. The analysis team captures the results of the OCTAVE in workshop notes, as well as in the Asset Profile Workbook, volume twelve of the OCTAVE Method Implementation Guide. Similar to NIST SP 800-30, the purpose of the OCTAVE final report is to gain management approval and sponsorship of increasing the organization's security posture based on the results of the risk assessment. Compiling the documentation prior to senior management review is part of the activities of OCTAVE process eight. The results of the management review are then documented, along with management approved protection strategy, risk mitigation plans, action list, and the next steps following the risk assessment. This documentation is then distributed to the senior managers, members of the analysis team, and other appropriate staff members.

3 Conclusions

During the course of this detailed comparative analysis, it has become clear to the authors that OCTAVE is fundamentally equivalent to best practices for an information security risk assessment as described by NIST SP 800-30, and OCTAVE Method Implementation Guidance provides an excellent tool to take the high-level recommendations and guidance found in NIST SP 800-30 to practices. OCTAVE's primary focus on risk assessment activities associated with risk management is an advantage if an organization needs detailed "how-to" instructions on performing and getting high value from an organizationally-led risk assessment. In explaining risk assessment roles and responsibilities, OCTAVE does not limit itself to a particular audience or technical skill set. Personnel inexperienced in assessing risk to information assets within their specific organizations are able to use guidance as explained in the OCTAVE Method Implementation Guides as a means to conduct an information security risk assessment in accordance with industry best practices.

Though OCTAVE can be tailored to fit the exact outline of NIST SP 800-30, the process of risk assessment is already very similar. The three major differentiators are the asset selection process, inclusion of likelihood in risk determination, and quantitative risk assessment guidance. OCTAVE concentrates primarily on critical assets as a means to direct managerial focus on those information assets that are most critical to the site's mission, as opposed to assessing risk on all information assets regardless of their criticality to the organization. OCTAVE does not include a means of factoring risk based on the likelihood that a particular technical vulnerability may be exploited. Since such probabilistic means of determining risk are inherent to a quantitative risk assessment, OCTAVE does not provide guidance for conducting quantitative information security risk assessments. However, OCTAVE does provide the flexibility to tailor the OCTAVE methodology in consideration of the incorporation of all three differentiators.

The bottom line from the comparison of OCTAVE to NIST SP 800-30 is that following the OCTAVE guidance will meet the spirit and intent of the NIST guidance for conducting the risk assessment as part of a total risk management program described in NIST SP 800-30.

4 References

Alberts, C. & Dorofee, A. (2001, June) Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) Method Implementation Guide, Version 2.0. Software Engineering Institute, Carnegie Mellon University.

Alberts, C. & Dorofee, A. (2001, December) OCTAVESM Criteria, Version 2.0. Software Engineering Institute, Carnegie Mellon University. Available from: <http://www.sei.cmu.edu/publications/documents/01.reports/01tr016.html>.

National Institute of Standards and Technology Special Publication 800-30, "Risk Management Guide for Information Technology Systems" (NIST SP 800-30), 2001

5 Glossary of Terms

Accountability (NIST) The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

Analysis Team (OCTAVE) An interdisciplinary team comprised of representatives of both the mission-related and information technology areas of the organization. The analysis team conducts the OCTAVE evaluation and analyzes the information. An analysis team consists of about three to five people, depending on the size of the organization and scope of the evaluation.

Asset (OCTAVE) Something of value to the enterprise. Information technology assets are a combination of logical and physical assets and are grouped into specific classes (information, systems, software, hardware, and people).

Asset Profile Workbook (OCTAVE) A consolidated set of worksheets and instructions to document the results of the OCTAVE processes for a specific critical asset. (The OCTAVE Asset Profile Workbook is *Volume 12: Asset Profile Workbook*.)

Assurance (NIST) Grounds for confidence that the four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. Adequately met includes: (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or bypass.

Availability (NIST) The security goal that generates the requirement for protection against:

- Intentional or accidental attempts to: (1) perform unauthorized deletion of data, or (2) otherwise cause a denial of service or data; and
- Unauthorized use of system resources.

Catalog of Practices (OCTAVE) A collection of good strategic and operational security practices that an organization can use to manage its security. (The OCTAVE Catalog of Practices is *Volume 15: Appendix A—OCTAVE Catalog of Practices*. Also available from: <http://www.sei.cmu.edu/publications/documents/01.reports/01tr020.html>)

Confidentiality (NIST) The security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and in transit.

Critical Assets (OCTAVE) The most important assets to an organization. The organization would suffer a large adverse impact if something happened to critical assets.

Denial of Service (NIST) The prevention of authorized access to resources or the delaying of time-critical operations.

Due Care (NIST) Managers and their organizations have a duty to provide for information security to ensure that the type of control, the cost of control, and the deployment of control are appropriate for the system being managed.

OCTAVE-Best Practices Comparative Analysis

Evaluation Criteria (OCTAVE) A set of qualitative measures against which a risk is evaluated. Evaluation criteria define high, medium, and low impacts for an organization.

Impact (OCTAVE) The effect of a threat on an organization's mission and business objectives.

Impact Value (OCTAVE) A qualitative measure of a risk's impact to the organization (high, medium, or low).

Integrity (NIST) The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has when it has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).

Information Asset (OCTAVE) Documented (paper or electronic) information or intellectual assets used to meet the mission of the enterprise.

IT-Related Risk (NIST) The net mission impact considering: (1) the probability that a particular threat source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability, and (2) the resulting impact if this should occur. IT-related risks arise from legal liability or mission loss due to:

- Unauthorized (malicious or accidental) disclosure, modification, or destruction of information;
- Unintentional errors and omissions;
- IT disruptions due to natural or man-made disasters; and/or
- Failure to exercise due care and diligence in the implementation and operation of the IT system.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Method (OCTAVE) Risk evaluation methodology developed by the Software Engineering Institute, Carnegie Mellon University, that was partially funded by the Defense Healthcare Information Assurance Program (DHIAP).

OCTAVE Method Implementation Guide (OMIG) (OCTAVE) The 18-volume set of manuals that document the processes, guidance, inputs, and outputs of the OCTAVE Method.

Operational Practice (OCTAVE) Security practices that focus on technology-related issues. They include issues related to how people use, interact with, and protect technology.

Organizational Vulnerability (OCTAVE) A weakness in organizational policy or practice that could result in unauthorized actions occurring. They are indications of missing or inadequate security practices.

Protection Strategy (OCTAVE) Defines the strategies that an organization uses to enable, initiate, implement, and maintain its internal security. It tends to incorporate long-term organization-wide values.

Risk (OCTAVE) The possibility of suffering harm or loss. It is the potential for realizing unwanted negative consequences of an event. Risk refers to a situation where a person could do

something undesirable or a natural occurrence could cause an undesirable outcome, resulting in a negative impact or consequence.

Risk (NIST) Within this document, synonymous with IT-Related Risk.

Risk Assessment (NIST) The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management is synonymous with Risk Analysis. **Risk Management (NIST)** The total process of identifying, controlling, and mitigating information system-related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.

Risk Management (OCTAVE) The ongoing process of identifying risks and implementing plans to address them.

Risk Mitigation Plan (OCTAVE) A plan that is intended to reduce the risks to a critical asset. Risk mitigation plans tend to incorporate actions or countermeasures designed to counter the threats to assets.

Risk Profile (OCTAVE) Defines the range of risks that can affect an asset. Risk profiles contain categories that are grouped according to threat source (human actors using network access, human actors using physical access, system problems, other problems).

Security (NIST) Information system security is a system characteristic and a set of mechanisms that span the system both logically and physically.

Security Goals (NIST) The five security goals are integrity, availability, confidentiality, accountability, and assurance.

Security Practice (OCTAVE) Actions that help initiate, implement, and maintain security within an organization. (Also called “Protection Strategy Practice.”)

Security Requirements (OCTAVE) Requirements outlining the qualities of information assets that are important to an organization. Typical security requirements are confidentiality, integrity, and availability.

Strategic Practice (OCTAVE) Security practices that focus on organizational issues at the policy level. They include business-related issues as well as issues that require organization-wide plans and participation.

Technology Vulnerability (OCTAVE) A weakness in systems that can directly lead to unauthorized action. Technology vulnerabilities are present in and apply to network services, architecture, operating systems, and applications. Types of technology vulnerabilities include design, implementation, and configuration vulnerabilities. (Note: also see “Organizational Vulnerability” and “Vulnerability.”)

Threat (NIST) The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

Threat (OCTAVE) An indication of a potential undesirable event. It refers to a situation in which a person could do something undesirable (e.g., an attacker initiating a denial-of-service

OCTAVE-Best Practices Comparative Analysis

attack against an organization's email server), or a natural occurrence could cause an undesirable outcome (e.g., a fire damaging an organization's information technology hardware). Threats have defined properties (asset, actor, motive, access, outcome).

Threat Profile (OCTAVE) Defines the range of threats that can affect an asset. Threat profiles contain categories that are grouped according to threat source: human actors using network access, human actors using physical access, system problems, and other problems.

Threat-source (NIST) Either: (1) intent and method targeted at the intentional exploitation of a vulnerability, or (2) a situation and method that may accidentally trigger a vulnerability.

Threat Analysis (NIST) The examination of threat-sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.

Vulnerability (NIST) A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the systems security policy. (Note: see also "Organizational Vulnerability" and "Technology Vulnerability.")

Vulnerability (OCTAVE) A weakness in an information system, system security practices and procedures, administrative controls, internal controls, implementation, or physical layout that could be exploited by a threat to gain unauthorized access to information or disrupt processing. There are two basic types of vulnerabilities—organizational and technology. (Note: see also "Organizational Vulnerability" and "Technology Vulnerability.")

Vulnerability Evaluation Approach (OCTAVE) An approach for evaluating each infrastructure component, including who will perform the evaluation and the tool(s) to be used.

| REPORT DOCUMENTATION PAGE | | | <i>Form Approved</i> <i>OMB No. 0704-0188</i> | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|---------------------------------------------------------------------------------------|--------------------------------------------------|----------------|
| 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 June 2003 | 3. REPORT TYPE AND DATES COVERED Comparative Analysis of OCTAVE and NIST SP 800-30 | | |
| 4. TITLE AND SUBTITLE OCTAVE-Best Practices Comparative Analysis: a comparison of the Operationally Critical Threat, Asset, and Vulnerability Evaluation SM (OCTAVE SM) Method and Commonly Accepted Best Practices for Assessing Information Security Risks as stated in The National Institute of Standards and Technology Special Publication 800-30 (NIST SP 800-30) | | 5. FUNDING NUMBERS DAMD17-99-C-9001 | | |
| 6. AUTHORS S. West, A. Andrews | | | | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Advanced Technology Institute 5300 International Blvd. N. Charleston, SC 29418 | | 8. PERFORMING ORGANIZATION REPORT NUMBER ATI IPT TR 03-4 | | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) USAMRAA 820 Chandler St. Ft. Detrick, MD 21702-5014 | | 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) Proper application of a valid risk assessment not only identifies risks in relation to business, it can also help build a corporate culture of appreciation for risk management throughout the organization. This report compares the information, guidance, and methods used to conduct a risk assessment of a site's critical assets as described in the <i>Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) Method Implementation Guide</i> with those of industry best practices and Federal guidelines as reflected in the National Institute of Standards and Technology Special Publication 800-30, <i>Risk Management Guide for Information Technology Systems (NIST SP 800-30)</i> . The OCTAVE Methodology is a focused, step-by-step guide to executing a risk assessment on an organization's most critical assets; NIST SP 800-30 provides broad guidance on risk assessment and risk management practices, defining the standard of commonly accepted best practices. This comparative analysis maps the nine steps of the risk assessment process recommended in NIST SP 800-30 to equivalent processes of OCTAVE. It indicates how well the OCTAVE risk assessment meets standards established by NIST SP 800-30 and provides recommendations about the usability of OCTAVE guidance for detailed "how-to" instructions on performing and realizing high value from an organization-led risk assessment. | | | | |
| 14. SUBJECT TERMS Information Security, Computer Security, Healthcare Information Systems, Risk Assessment, Risk Analysis, Vulnerability Evaluation, HIPAA, OCTAVE, NIST SP 800-30 | | 15. NUMBER OF PAGES 26 | | 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 UNLIMITED | |