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.

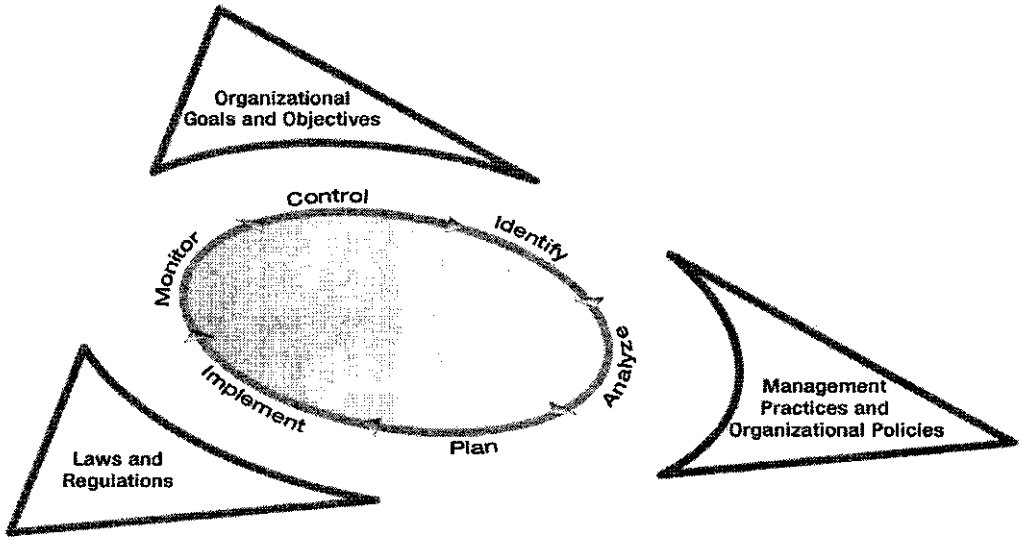

Figure 1: Risk Management Process Within the Organizational Context

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 that 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:[1]

- 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 under protecting 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.

[1] 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.

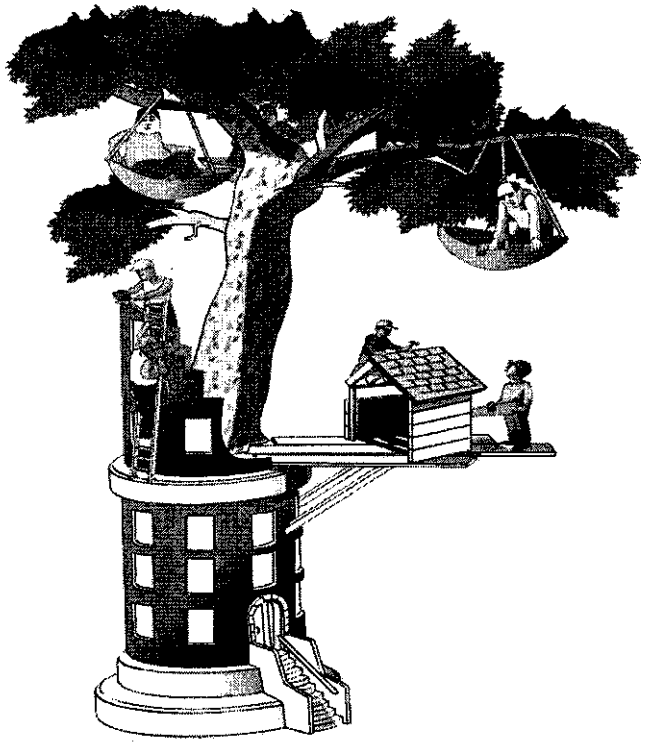

Figure 2: Results of an Unbalanced Security Risk Management Process

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®-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.

® 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.

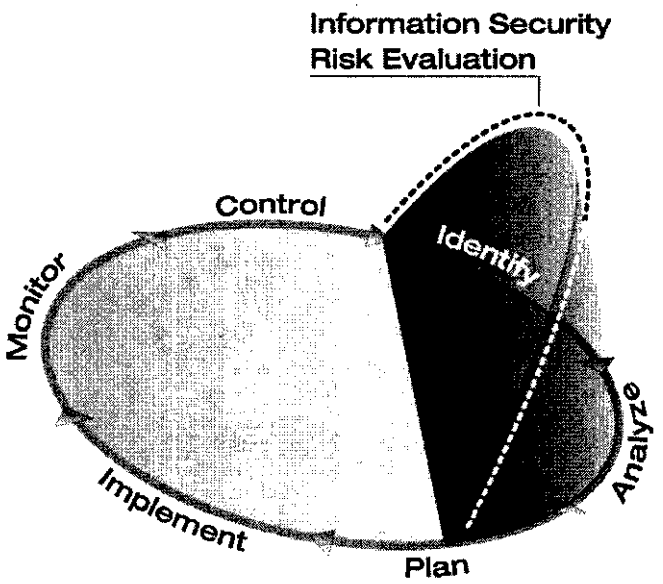

Figure 3: Information Security Risk Evaluation Within an Information Security Risk Management Process

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 12th 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].