Risk-Centered Practices

Julia H. Allen

October 2006

ABSTRACT: This article establishes the role that risk management and risk assessment play in determining what security practices to implement and in what order. Risk management is critical in sustaining an acceptable level of security, given that it is not possible to be 100% secure.

INTRODUCTION

Why Are Risk-Centered Practices Necessary?

Given that it is impractical (and probably impossible) to ensure that an operational system is 100% secure at any point in time, security practitioners have found it useful to adopt risk management and assessment strategies to determine which security practices to deploy.

Risk assessment results are identified as a key prerequisite for sustainable operational security in Plan, Do, Check, Act, Table 1. This topic is described in more detail in the BSI Risk Management and Architectural Risk Analysis content areas and applied to deployment and operations here.

Definition of Risk

Alberts [Alberts 05] defines risk as "the possibility of suffering harm or loss." Jones [Jones 05] defines risk as "the probable frequency and probable magnitude of future loss." NIST's Special Publication Risk Management Guide for Information Technology Systems states the following [Stoneburner 02]:

> *Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.*
>
> *Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions.*

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Phone: 412-268-5800
Toll-free: 1-888-201-4479

www.sei.cmu.edu

Questions to Ask

In determining what risk-centered practices need to be deployed to ensure a more sustainable level of security, practitioners (and their managers) need to ask and answer the following questions [Allen 05; BSI Governance & Management article "How Much Security Is Enough?"]:

- What is the value we need to protect?
- To sustain this value, what software, system, and information assets need to be protected? Why do they need to be protected? What happens if they’re not protected?
- What potential adverse conditions and consequences need to be prevented and managed? At what cost? How much disruption can we stand before we take action?
- How do we determine and effectively manage residual risk (the risk remaining after mitigation actions are taken)?
- How do we integrate our answers to these questions into an effective, implementable, enforceable security strategy and plan?

Principles that Argue for a Risk-Centered Approach

NIST Special Publication 800-27, Engineering Principles for Information Technology Security [Stoneburner 04] identifies 33 principles for IT security, 7 of which are essential for deploying and operating a system using risk-centered practices. The 800-27 principle numbers are retained here to ease traceability to the publication:

- "Principle 5: **Reduce risk to an acceptable level.** The goal is to enhance mission/business capabilities by mitigating mission/business risk to an acceptable level. (See also BSI Governance & Management article "How Much Security Is Enough?" for a discussion of risk tolerance).
- Principle 6: **Assume that external systems are insecure.** Those responsible for deployment and operations should presume the security measures of an external system are different from those of a trusted internal system and deploy security practices accordingly.
- Principle 7: **Identify potential tradeoffs between reducing risk, increased costs, and decreased operational effectiveness.** A cost-benefit analysis should be conducted for each proposed security control. In some cases, the benefits of a more secure system may not justify the costs. In modifying or adjusting security goals, an acceptance of greater risk and cost may be inevitable.
- Principle 8: Implement tailored system security measures to meet organizational security goals. Implement lower assurance solutions with lower costs

to protect less critical systems and higher assurance solutions only for the most critical assets.

- Principle 9: **Protect information while being processed, in transit, and in storage.** Select security measures that protect the confidentiality, integrity, and availability of information in all of these states.
- Principle 10: **Consider custom products to achieve adequate security.** In some instances, commercially available products may not be sufficient.
- Principle 11: **Protect against all likely classes of "attacks."** Examples include passive monitoring, active network attacks, insider threat, attacks requiring physical access, social engineering, and the insertion of malicious code during software development and distribution."

Risk-Centered Practices

Identifying the organization's most critical assets and where those assets are most at risk should inform the selection and prioritization of security practices for deployment and operations.

Risk-centered practices that aid in security practice selection for deployment and operations include the following. These are listed in the order recommended for implementation.

1. Define the scope of the risk assessment. Ensure a clear and direct tie to business and mission objectives.
2. Identify information and software assets that are important to the organization. Focus risk assessment on those assets judged to be the most critical.
3. Identify asset owners and custodians.
4. Determine the criteria for accepting risks and the acceptable levels of risk, often referred to as risk tolerances or risk thresholds.
5. Identify the relationships among critical assets, the threats to those assets, and vulnerabilities (both organizational and technological) that can expose assets to threats.
6. Assess the likelihood of threats and vulnerabilities.
7. Identify the impacts due to losses resulting from realized risks.
8. Identify risks and evaluate options for treatment of risks (accept, mitigate, avoid, transfer, share with a third party (such as a supplier)).
9. Identify practice-based protection strategies (control objectives and controls) that reduce risks to critical assets to levels that are within acceptable tolerances. Controls can be deployed to reduce likelihood and impact.
10. Identify potential tradeoffs between reducing risk, increased costs, and decreased operational effectiveness.

11. Identify approaches for managing residual risks that remain after protection strategies are adopted.
12. Measure, review, and revise risk-centered practices. Re-assess risks periodically.

Table 1 (included at the end of this article) provides additional details and sources that expand these practices.

DESCRIPTION OF SOURCES

The following sources were used to identify the risk-centered practices described above and expanded in Table 1.

BS 7799-3

British Standard 7799-3 Guidelines for information security risk management [BSI 06] defines in detail the risk management practices identified in ISO 27002/17799 [ISO 05a] and ISO 27001 [ISO 05b]. It states the following in its introduction:

> *A process approach (for assessing risks, treating risks, and ongoing risk monitoring, risk reviews, and re-assessments) emphasizes the importance of (a) understanding business information security requirements and the need to establish policy and objectives for information security; (b) selecting, implementing, and operating controls in the context of managing an organization's overall business risks; (c) monitoring and reviewing the performance and effectiveness of the Information Security Management System (ISMS)*[1] *to manage business risks; (d) continual improvement based on objective risk measurement.*

BS 7799-3 includes useful information identifying categories of information security and organizational risk in Annex B and examples of assets, threats, vulnerabilities, and risk assessment methods in Annex A.

FIPS 199

With respect to identifying and categorizing information-related assets, NIST's Standards for Security Categorization of Federal Information and Information Systems provides useful guidance to establish security categories for both infor-

[1] Defined in [ISO 05b].

mation and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization [NIST 04].

ISO/IEC 27005

This standard [ISO 08] defines a Plan, Do, Check, Act information security risk management process, consisting of the following steps:

Plan

1. **Establish the context** for information security risk management. This includes selecting criteria for evaluating risk, determining impact, and accepting risk; defining the asset scope and boundaries over which risk management will be conducted (for example, which applications will be assessed); and determining the organizational structure, roles, and responsibilities for performing risk management. (Clause 7)
2. **Risk assessment** involves conducting risk analysis to identify risks in terms of assets and their value, threats, existing controls, vulnerabilities that could be exploited, and consequences due to impact and loss should risks be realized. The magnitude of potential consequences is estimated in qualitative terms, quantitative where possible, taking the likelihood of incident occurrence into account. Risks are prioritized against evaluation criteria and organizational objectives. (Clause 8)
3. **Develop a risk treatment plan** that identifies the controls necessary to reduce, retain, avoid, or transfer identified risks. Controls are selected by performing a cost/benefit analysis, taking criteria into account. Residual risk falls within acceptable risk tolerances. (Clause 9)
4. The decision to **accept identified risks** and the responsibilities for each decision are formally documented. Responsible managers review and approve proposed risk treatment plans. (Clause 10) Risk information is shared between decision makers and key stakeholders to provide assurance and support ongoing decision making. (Clause 11)

Do

5. Implement the risk treatment plan.

Check

6. Continually monitor and review risks including all relevant factors (including asset value, impacts, threats, vulnerabilities, and likelihood). Identify

and act on any changes that add new assets, threats, and vulnerabilities or that update existing risk dimensions, priorities, and treatment. (Clause 12)

Act

7. Maintain and improve the information risk management process through ongoing monitoring and review. (Clause 12)

OCTAVE and OCTAVE Allegro

OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM) is a method for managing information security risks. Unlike technology-focused assessments (such as vulnerability assessments or penetration tests), "OCTAVE is targeted at organizational risk and focused on strategic, practice-related issues. The intent of OCTAVE is to strike a balance between operational risk, security practices, and technology" [Alberts 03].

The **three phases** of OCTAVE are

- Phase 1: Build Asset-Based Threat Profiles
  - Process 1: Identify senior management knowledge.
  - Process 2: Identify operational area knowledge.
  - Process 3: Identify staff knowledge.
  - Process 4: Create threat profiles.
- Phase 2: Identify Infrastructure Vulnerabilities
  - Process 5: Identify key components.
  - Process 6: Evaluate selected components.
- Phase 3: Develop Security Strategy and Plans
  - Process 7: Conduct risk analysis.
- Process 8: Develop protection strategy.

OCTAVE Allegro is a more streamlined approach that "optimizes the process of assessing information security risks to that an organization can obtain sufficient results with a small investment in people, time, and other limited resources" [Caralli 07]. Allegro focuses primarily on the use, storage, transport, and processing of information assets, and asset exposure to threats, vulnerabilities, and disruptions.

Allegro has the following eight steps:

Establish Drivers

1. Establish risk measurement criteria

Profile Assets

2. Develop an information asset profile
3. Identify information asset containers

Identify Threats

4. Identify areas of concern
5. Identify threat scenarios

Identify and Mitigate Risks

6. Identify risks
7. Analyze risks
8. Select mitigation approach

Software Security: Building Security In

Chapter 2 of the book Software Security: Building Security In describes a risk management framework (RMF) comprising five stages [McGraw 06]:

1. Understand the business context.
2. Identify the business and technical risks.
3. Synthesize and rank the risks.
4. Define the risk mitigation strategy.
5. Carry out fixes and validate.

This chapter also presents a comprehensive example of applying RMF to a server application with stringent first-to-market delivery date requirements, high availability requirements (99.999% uptime), and 100% transaction accuracy requirements to meet federal regulations.

IMPLEMENTATION CONSIDERATIONS

Risk-centered practices represent the state of practice for some organizations and systems. Field work in using the OCTAVE method[2] has shown that if a risk assessment is performed at a mid-level in the organization, localized decisions can

[2] Some OCTAVE experience reports are available on the CERT Web site (http://www.cert.org/octave/).

be made and acted on. Occasionally there are barriers to extrapolating these decisions to an organizational or system-wide level, which is often required to sustain successful improvement at the local level. An example is the need for a policy on incident reporting that enables local action but needs to be authored and sponsored at a broader organizational level to be enforceable.

If the organization performing system deployment and operations has no framework in which to accept localized risk assessment findings and deploy risk mitigation strategies to benefit the entire organization (and system), sustained improvement may be problematic. That said, an effective way to get started with risk-centered practices is described in the GAO's report Information Security Risk Assessment: Practices of Leading Organizations:

Rather than conducting one large risk assessment covering all of an entity's operations at once, the organizations generally conducted a series of narrower assessments on various individual segments of the business. As a result, the scope of each assessment was limited to a particular business unit, system, or facility, or to a logically related set of operations [GAO 99].

CONCLUSION

Risk-centered practices assume the presence of an appropriate risk assessment method, selected to satisfy business objectives and security, legal, and regulatory requirements. The selected risk assessment method should ensure that subsequent assessments "produce comparable and reproducible results" [ISO 05b].

To be effective and sustainable, risk-centered practices must be deployed using a continuous, plan-do-check-act approach through the useful life of the system.

Table 1: Risk-Centered Practices that Aid in Security Practice Selection for Deployment and Operations

Table 1 lists risk-centered practices and pointers to sources that provide detailed descriptions and implementation guidance. Practices are listed in the order recommended for implementation. Each source is fully cited on its first occurrence and summarized thereafter.

Table 1. Risk-centered practices that aid in security practice selection for deployment and operations

Practice	Sources

Define the scope of the risk assessment. Ensure a clear and direct tie to business and mission objectives.	• “Introduction to the OCTAVE® Approach” [Alberts 03]; OCTAVE Allegro [Caralli 07] • Software Security:Building Security In, Chapter 2, “A Risk Management Framework” [McGraw 06] • ISO 27005 Information Security Risk Management [ISO 08]
Identify information assets that are important to the organization. Focus risk assessment on those assets judged to be the most critical: • asset value • business and legal requirements • impact of loss of confidentiality, integrity, availability	• FIPS 199 Security Categorization of Federal Information and Information Systems [NIST 04] • Software Security, Chapter 2 [McGraw 06] • BS 7799-3 Guidelines for information security risk management [BSI 06] • ISO 27005 [ISO 08] • OCTAVE [Alberts 03]; OCTAVE Allegro [Caralli 07]
Identify asset owners and custodians.	• FIPS 199 [NIST 04] • BS 7799-3 [BSI 06] • ISO 27001 Information security management systems [ISO 05b]
Determine the criteria for accepting risks and the acceptable levels of risk, often referred to as risk tolerances or risk thresholds.	• BS 7799-3 [BSI 06] • ISO 27005 [ISO 08] • ISO 27001 [ISO 05b]
Identify the relationships among critical assets, the threats to those assets, and vulnerabilities (both organizational and technological) that can expose assets to threats.	• OCTAVE [Alberts 03]; OCTAVE Allegro [Caralli 07] • BS 7799-3 [BSI 06] • Software Security, Chapter 2 [McGraw 06] • ISO 27005 [ISO 08] • ISO 27001 [ISO 05b]

Assess the likelihood of threats[3] and vulnerabilities.	• OCTAVE [Alberts 03]; OCTAVE Allegro [Caralli 07] • BS 7799-3 [BSI 06] • Software Security, Chapter 2 [McGraw 06] • ISO 27005 [ISO 08]
Identify the impacts due to losses resulting from realized risks.	• OCTAVE [Alberts 03]; OCTAVE Allegro [Caralli 07] • BS 7799-3 [BSI 06] • Software Security, Chapter 2 [McGraw 06] • ISO 27005 [ISO 08] • ISO 27001 [ISO 05b]
Identify risks and evaluate options for treatment of risks (accept, mitigate, avoid, transfer, share with a third party (such as a supplier)).	• BS 7799-3 [BSI 06] • OCTAVE [Alberts 03]; OCTAVE Allegro [Caralli 07] • ISO 27005 [ISO 08] • ISO 27001 [ISO 05b]
Identity practice-based protection strategies (control objectives and controls) that reduce risks to critical assets to levels that are within acceptable tolerances. Controls can be deployed to reduce likelihood and impact.	• OCTAVE [Alberts 03]; OCTAVE Allegro [Caralli 07] • BS 7799-3 [BSI 06] • Software Security, Chapter 2 [McGraw 06] • ISO 27001 [ISO 05b] • ISO 27005 [ISO 08]
Identify potential tradeoffs between reducing risk, increased costs, and decreased operational effectiveness	• NIST 800-27 (Principle 7) Engineering Principles for Information Technology Security [Stoneburner 04] • ISO 27005 [ISO 08]

[3] Threats include characterizing an organization's "adversaries, their potential motivations, and their classes of attack" http://nsa2.www.conxion.com/support/guides/sd-1.pdf.

Identify approaches for managing residual risks that remain after protection strategies are adopted.	• BS 7799-3 [BSI 06] • ISO 27005 [ISO 08]
Measure, review, and revise risk-centered practices. Take into account changes to the organization, business objectives and processes, regulatory and marketplace factors, threats, technology, and control effectiveness. Re-assess risks periodically.	• BS 7799-3 [BSI 06] • Software Security, Chapter 2 [McGraw 06] • ISO 27001 [ISO 05b] • ISO 27005 [ISO 08]

REFERENCES

[Alberts 05] Alberts, Christopher & Dorofee, Audrey. Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments (CMU/SEI-2005-TN-032). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2005.

[Alberts 03] Alberts, Christopher; Dorofee, Audrey; Stevens, James; & Woody, Carol. “Introduction to the OCTAVE®Approach.” Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003.

[Allen 05] Allen, J. Governing for Enterprise Security (CMU/SEI-2005-TN-023). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2005.

[BSI 06] British Standards Institute. Information security management systems – Part 3: Guidelines for information security risk management. BS 7799-3:2006. BSI, March 17, 2006.

[Caralli 07] Caralli, Richard; Stevens, James; Young, Lisa; Wilson, William. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. CMU/SEI-2007-TR-012. Carnegie Mellon University, Software Engineering Institute, May 2007.

[GAO 99] U.S. Government Accounting Office. Information Security Risk Assessment: Practices of Leading Organizations (GAO/AIMD-00-33). November 1999.

[ISO 08] International Organization for Standardization. Information technology – Security techniques –Information security risk management. ISO/IEC 27005, First edition, June 15, 2008. Cancels and replaces ISO/IEC TR 13335-3:1998 and ISO/IEC TR 13335-4:2000.

[ISO 05a] International Organization for Standardization. Information technology – Security techniques – Code of practice for information security management. ISO/IEC 27002:2005, June 2005. Also known as ISO/IEC 17799:2005.

[ISO 05b] International Organization for Standardization. Information technology – Security techniques – Information security management systems – Requirements. ISO/IEC 27001:2005(E), First edition, October 15, 2005.

[Jones 05] Jones, Jack. “An Introduction to Factor Analysis of Information Risk (FAIR): A framework for understanding, analyzing, and measuring information risk.” Jack A. Jones, 2005.

[McGraw 06] McGraw, Gary. Software Security: Building Security In. Boston, MA: Addison-Wesley, 2006. For Article 2, refer to Chapter 2, “A Risk Management Framework.” For Articles 3 and 4, refer to Chapter 9, “Software Security Meets Security Operations.”

[NIST 04] National Institute of Standards and Technology. Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199). Federal Information Processing Standards Publication, NIST, February 2004.

[Stoneburner 04] Stoneburner, Gary; Hayden, Clark; & Feringa, Alexis. Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A (NIST Special Publication 800-27, Revision A). National Institute of Standards and Technology, June 2004.

[Stoneburner 02] Stoneburner, Gary; Goguen, Alice; & Feringa, Alexis. Risk Management Guide for Information Technology Systems (NIST Special Publication 800-30). National Institute of Standards and Technology, July 2002.

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

DM-0001120