Software Engineering Institute | Carnegie Mellon University

Deployment and Operations References

Julia H. Allen

October 2006

BIBLIOGRAPHY

[ACC 02] American Chemistry Council. *Implementation Guide for Responsible Care® Security Code of Management Practices: Site Security and Verification*, 2002.

[ACC 06] American Chemistry Council’s Chemical Information Technology Council. “Guidance for Addressing Cyber Security in the Chemical Industry, Version 3.0.” ACC *ChemITC*, May 2006.

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

[Alberts 04] Alberts, Christopher; Dorofee, Audrey; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. *Defining Incident Management Processes for CSIRTs: A Work in Progress* (CMU/SEI-2004-TR-015). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004.

[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.

[Allen 01] Allen, Julia. *The CERT Guide to System and Network Security Practices*. Boston, MA: Addison Wesley, 2001.

[Allen 03] Allen, Julia; Gabbard, Derek’ & May, Christopher. *Outsourcing Managed Security Services* (CMU/SEI-SIM-012). 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.

[Bowen 06] Bowen, Pauline; Hash, Joan; Wilson, Mark. Information Security Handbook: A Guide for Managers. (NIST Special Publication 800-100). Gaithersburg, MD: National Institute of Standards and Technology, October 2006.

[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.

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

[Campbell 05] Campbell, Philip. “A COBIT Primer.” Sandia Report SAND2005-3455. Sandia National Laboratories, June 2005.

[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.

[CERT 05] CERT. *Survivability and Information Assurance Curriculum*. Software Engineering Institute, Carnegie Mellon University, 2005. Most of the material in this article description is taken from the curriculum overview.

[CERT 08] CERT. “Making Information Security Policy Happen.” CERT's Podcast Series: Security for Business Leaders, June 2008.

[CERT 08a] "Insider Threat Research," Pittsburgh, PA: CERT, Software Engineering Institute, Carnegie Mellon University, 2008.

[Chew 08] Chew, Elizabeth; Swanson, Marianne; Stine, Kevin; Bartol, Nadya; Brown, Anthony; & Robinson, Will. *Performance Measurement Guide for Information Security*. NIST Special Publication 800-55, Revision 1. Gaithersburg, MD: National Institute of Standards and Technology, July 2008.

[CGTF 04] Corporate Governance Task Force. “Information Security Governance: A Call to Action.” National Cyber Security Partnership, April 2004.

[CIS 08] "The Center for Internet Security." 2008.

[CISWG 04] Corporate Information Security Working Group. Adam H. Putnam, Chairman; Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census Government Reform Committee, U.S. House of Representatives. “Report of the Best Practices and Metrics Teams.” November 17, 2004; updated January 10, 2005.

[COBIT 08] Wikipedia. "COBIT." 2008.

[Conner 06] Conner, Bill. “On compliance: Get a step-by-step plan for meeting PCI standards.” *SC Magazine*, August 7, 2006.

[CSCSP 06] Chemical Sector Cyber Security Program. “Guidance for Addressing Cyber Security in the Chemical Industry, Version 3.0.” American Chemistry Council, Chemical Information Technology Council, May 2006.

[CVE 08] National Cyber Security Division of the U.S. Department of Homeland Security. Common Vulnerabilities and Exposures," 2008.

[DiD 08] Wikipedia. "Defense in Depth." 2008.

[FFIEC 06] Federal Financial Institutions Examination Council. *IT Examination Handbook: Information Security.* July 2006.

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

[Goertzel 08] Goertzel, Karen Mercedes; Winograd, Theodore. *Enhancing the Development Life Cycle to Produce Secure Software, Version 2*. U.S. Department of Homeland Security, October 2008.

[Guel 01] Guel, Michele D. "A Short Primer for Developing Security Policies." *The SANS Policy Primer*. The SANS Institute, 2001.

[Hazlewood 06] Hazlewood, Victor. *Defense-In-Depth: An Information Assurance Strategy for the Enterprise*. La Jolla, CA: San Diego Supercomputer Center Security Technologies, 2006.

[IIA 05] The Institute of Internal Auditors. *Global Technology Audit Guides: Change and Patch Management Controls: Critical for Organizational Success*. July 2005.

[IsecT 06] IsecT Ltd. Other security standards (2006).

[ISF 07] Information Security Forum. *The Standard of Good Practice for Information Security,* 2007.

[ISO 97] International Organization for Standardization. *Information technology – Guidelines for the management of IT Security – Part 2: Managing and planning IT Security.* ISO/IEC TR 13335-2:1997(E), December 15, 1997.

[ISO 04] International Standards Organization. *Information Technology – Systems Security Engineering – Capability Maturity Model® (SSE-CMM®).* ISO/IEC 21827:2002. Also available through The International Systems Security Engineering Association (ISSEA).

[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.

[ISO 05c] International Organization for Standardization. *Information technology – Service management* (ISO/IEC 20000-1:2005(E)), First edition, December 15, 2005. *Part 2: Code of practice* (ISO/IEC 20000-2:2005(E)), December 15, 2005.

[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.

[ITGI 07a] Information Technology Governance Institute. *COBIT 4.1 Control Objectives for Information and related Technology*. ITGI, 2007. http://www.itgi.org and http://www.isaca.org.

[ITGI 07b] Information Technology Governance Institute. *COBIT Security Baseline: An Information Security Survival Kit, 2nd ed*. http://www.itgi.org/ (2007).

[ITGI 08] IT Governance Institute & Office of Government Commerce. “Aligning COBIT®, ITIL®, and ISO 17799 for Business Benefit: A Management Briefing from ITGI and OGC.” ITGI & OGC, 2008.

[ITIL 99] IT Infrastructure Library. *Security Management*. Norwich, Norfolk, England: Office of Government Commerce, 1999.

[ITIL 00] IT Infrastructure Library. *Service Support*. Norwich, Norfolk, England: Office of Government Commerce, 2000.

[ITIL 01] IT Infrastructure Library. *Service Delivery*. Norwich, Norfolk, England: Office of Government Commerce, 2001.

[ITIL 08] Wikipedia. "Information Technology Infrastructure Library." 2008.

[ITPI 04] Behr, Kevin; Kim, Gene; & Spafford, George. *Visible Ops Handbook: Starting ITIL in Four Practical Steps*. IT Process Institute, 2004. Introductory and ordering information is available at http://www.itpi.org.

[ITPI 08] Kim, Gene; Love, Paul; & Spafford, George. *Visible Ops Security: Achieving Common Security and IT Operations Objectives in 4 Practical Steps*. IT Process Institute, 2008. Introductory and ordering information is available at http://www.itpi.org.

[itSMF 07] The IT Service Management Forum. “An Introductory Overview of ITIL® V3.” itSMF Ltd., 2007.

[Kim 04] Kim, Gene & Allen, Julia. “High-Performing IT Organizations: What You Need to Change to Become One.” *BetterManagement.com*, April 30, 2004.

[Kim 06] Kim, Gene, et al. *IT Controls Performance Study: Identification of foundational controls that have the greatest impact on IT operations, security, and audit performance measures*. IT Process Institute, 2006. Ordering information is available at http://www.itpi.org/home/performance_study.php.

[Kissel 08] Kissel, Richard; Stine, Kevin; Scholl, Matthew; Rossman, Hart; Fahlsing, Jim; & Gulick, Jessica. Security Considerations in the Information System Development Life Cycle. (NIST Special Publication 800-64, Revision 2). National Institute of Standards and Technology, March 2008.

[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.

[Lindner 06] Lindner, Martin; Losi, Stephanie; & Allen, Julia. "Proactive Remedies for Rising Threats." CERT Podcast Series: Security for Business Leaders. August 2006.

[May 06] May, Christopher J.; Hammerstein, Josh; Mattson, Jeff; & Rush, Kristopher. *Defense-in-Depth: Foundations for Secure and Resilient Enterprises* (CMU/SEI-2006-HB-003). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2006.

[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."

[NIAC 05] National Infrastructure Advisory Council. "Risk Management Approaches to Protection; Final Report and Recommendations by the Council." NIAC, October 11, 2005.

[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.

[NIST 06] National Institute of Standards and Technology. *Minimum Security Requirements for Federal Information and Information Systems* (FIPS PUB 200). Federal Information Processing Standards Publication, NIST, March 2006.

[NSA] National Security Agency. "Defense in Depth: A Practical Strategy for Achieving Information Assurance in Today's Highly Networked Environments."

[NSA 06] National Security Agency. "The 60 Minute Network Security Guide (First Steps Towards a Secure Network Environment), Version 2.1." National Security Agency, May 15, 2006.

[OGC 07] Office of Government Commerce. *ITIL®[1] (Information Technology Infrastructure Library) Lifecycle Publication Suite, Version 3*. Office of Government Commerce, Stationery Office, July 30, 2007. Refer to http://www.itsmfi.org.

[1] ITIL is a registered trademark of OGC.

[PCI 08] Payment Card Industry (PCI) Data Security Standard, Version 1.2, PCI Security Standards Council, October 2008.

[Ravenel 06] Ravenel, J. Patrick. “Effective Operational Security Metrics.” *Information Systems Security 15*, 3 (July/August 2006).

[Rogers 02] Rogers, Lawrence R. & Allen, Julia. “Securing Information Assets - Security Knowledge in Practice.” *Crosstalk: The Journal of Defense Software Engineering*, November 2002.

[Rogers 04] Rogers, Lawrence R. “Principles of Survivability and Information Assurance.” Software Engineering Institute, Carnegie Mellon University, 2004.

[Ross 06] Ross, Ron. "Managing Enterprise Risks in Today's World of Sophisticated Threats: A Framework for Developing Broad-Based, Cost-Effective Information Security Programs." National Institute of Standards and Technology, November 2006.

[Ross 07a] Ross, Ron. "Managing Enterprise Security Risk with NIST Standards." *Computer* magazine, IEEE Computer Society, August 2007.

[Ross 07b] Ross, Ron; Katzke, Stu; Johnson, Arnold; Swanson, Marianne; Stoneburner, Gary; Rogers, George; & Lee, Annabelle. *Recommended Security Controls for Federal Information Systems* (NIST Special Publication 800-53, Revision 2). National Institute of Standards and Technology, December 2007.

[Scott 01] Scott, Donna. “Network and System Management: Often the Weakest Link in Business Availability.” Gartner, July 3, 2001.

[Stern 01] Stern, Andrea. “Reinvesting the IT Dollar: From IT Firefighting to Quality Strategic Services.” *EDUCAUSE Quarterly*, Number 3, 2001.

[Stevens 93] Stevens, W. Richard. *TCP/IP Illustrated, Volume 1: The Protocols*. Boston, MA: Addison-Wesley, 1993.

[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.

[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.

[Swanson 06] Swanson, Marianne; Hash, Joan; & Bowen, Pauline. *Guide for Developing Security Plans for Federal Information Systems* (NIST Special Publication 800-18, Revision 1). National Institute of Standards and Technology, February 2006.

[Visa 07] Visa U.S.A. Inc. "Visa U.S.A Cardholder Information Security Program Payment Application Best Practices, Version 1.4." January 2007.

[Wikipedia-PCI 08] Wikipedia. "Payment Card Industry." 2008.

[Womack 91] Womack, James P.; Jones, Daniel T.; & Roos, Daniel. *The Machine That Changed the World: The Story of Lean Production*. New York, NY: Harper Perennial, 1991.

[Worthen 05] Worthen, Ben. “ITIL Power.” *CIO Magazine*, September 1, 2005.

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.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0001120