



Governance and Management References

Julia H. Allen

November 2009

BIBLIOGRAPHY

[ACC 2002]

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

[ACC 2006]

American Chemistry Council's Chemical Information Technology Council. *Guidance for Addressing Cyber Security in the Chemical Industry, Version 3.0*. ACC ChemITC Chemical Sector Cyber Security Program, May 2006.

[AESRM 2005]

The Alliance for Enterprise Security Risk Management. *Convergence of Enterprise Security Organizations*. Booz Allen Hamilton, November 8, 2005.

[Alberts 2002]

Alberts, Christopher & Dorofee, Audrey. *Managing Information Security Risks: The OCTAVE Approach*. New York: Addison Wesley, 2002.

[Allen 2005]

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

[Allen 2007]

Allen, Julia & Westby, Jody R. "Characteristics of Effective Security Governance." *Governing for Enterprise Security (GES) Implementation Guide* (CMU/SEI-2007-TN-020). Software Engineering Institute, Carnegie Mellon University, 2007.

[Allen 2008]

Allen, Julia; Barnum, Sean; Ellison, Robert; McGraw, Gary; & Mead, Nancy. *Software Security: A Guide for Project Managers*. Addison-Wesley, 2008.

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

[Bowen 2006]

Bowen, Pauline; Hash, Joan; & Wilson, Mark. *Information Security Handbook: A Guide for Managers* (NIST Special Publication 800-100). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2006.

[BRT 2004]

Business Roundtable. *Securing Cyberspace: Business Roundtable's Framework for the Future*. Business Roundtable, May 2004.

[BRT 2005]

Business Roundtable. *Committed to Protecting America: CEO Guide to Security Challenges*. February 2005 (released May 2005).

[Caralli 2004a]

Caralli, Richard. *The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management* (CMU/SEI-2004-TR-010). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004.

[Caralli 2004b]

Caralli, Richard. *Managing for Enterprise Security* (CMU/SEI-2004-TN-046). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004.

[Caralli 2006]

Caralli, Richard. *Sustaining Operational Resiliency: A Process Improvement Approach to Security Management* (CMU/SEI-2006-TN-009). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2006.

[Caralli 2007]

Caralli, Richard; Stevens, James. F.; Wallen, Charles M.; White, David W.; Wilson, William R.; & Young, Lisa R. *Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes* (CMU/SEI-2007-TR-009). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2006.

[Carey 2005]

Carey, Mark. *Enterprise Risk Management: How To Jumpstart Your Implementation Efforts*. International Risk Management Institute, 2005.

[CERT 2009]

CERT Resilient Enterprise Management Team. *CERT Resiliency Management Model, v1.0*. Software Engineering Institute, Carnegie Mellon University, 2009.

[CGTF 2004]

Corporate Governance Task Force. *Information Security Governance: A Call to Action*. National Cyber Security Partnership, April 2004.

[COSO 2004]

The Committee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management-Integrated Framework*. Committee of Sponsoring Organizations of the Treadway Commission, September 2004.

[Deloitte 2007]

Deloitte Touche Tohmatsu. *2007 Global Security Survey*. Deloitte Touche Tohmatsu, 2007.

[Howard 2006]

Howard, Michael & Lipner, Steve. *The Security Development Lifecycle--SDL: A Process for Developing Demonstrably More Secure Software*. Redmond, WA: Microsoft Press, 2006.

[IIA 2000]

The Institute of Internal Auditors. *Information Security Management and Assurance: A Call to Action for Corporate Governance*. IIA and Critical Information Assurance Project, 2000.

[IIA 2001a]

The Institute of Internal Auditors. *Information Security Governance: What Directors Need to Know*. IIA, 2001.

[IIA 2001b]

The Institute of Internal Auditors. *Building, Managing, and Auditing Information Security*. IIA, 2001.

[ITGI 2006]

IT Governance Institute. *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*. ITGI, 2006.

[Jones 2005]

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 2006]

McGraw, Gary. *Software Security: Building Security In*. Boston, MA: Addison-Wesley, 2006.

[McGraw 2009]

McGraw, Gary; Chess, Brian; & Miguez, Sammy. *Building Security In Maturity Model BSIMM v1.0*. 2009

[Moulton 2003]

Moulton, Rolf & Coles, Robert. "Applying information security governance." *Computers & Security* 22, 7, Elsevier Ltd., 2003.

[NIAC 2005]

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

[Nolan 2005]

Nolan, Richard & McFarlan, F. Warren. "Information Technology and the Board of Directors." *Harvard Business Review*, October 2005.

[OECD 2003]

Organisation for Economic Co-Operation and Development. *Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. OECD, 2003.

[PCI 2009a]

Payment Card Industry Security Standards Council. *Payment Card Industry (PCI) Data Security Standard, Version 2.0*. PCI Security Standards Council, July 2009.

[PCI 2009b]

PCI Security Standards Council. *Payment Card Industry (PCI) Payment Application Data Security Standard, Requirements and Security Assessment Procedures, Version 2.0*. PCI Security Standards Council, July 2009.

[Steven 2006]

Steven, John. "Adopting an Enterprise Software Security Framework." *IEEE Security & Privacy* 4, 2 (March-April 2006): 84-87.

[Tribbensee 2003]

Tribbensee, Nancy E. "Liability for Negligent Security: Implications for Policy and Practice," Ch. 4, 45-57. *Computer and Network Security in Higher Education*. Edited

by Mark Luker & Rodney Petersen. San Francisco, CA: Jossey-Bass, Inc., EDUCAUSE Leadership Strategies, 2003.

[Westby 2005]

Westby, Jody, ed. "[Roadmap to an Enterprise Security Program](#)." American Bar Association, Privacy & Computer Crime Committee, Section of Science & Technology Law. American Bar Association, 2005.

[Westby 2007]

Westby, Jody R. & Allen, Julia H. *Governing for Enterprise Security (GES) Implementation Guide* (CMU/SEI-2007-TN-020). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, August 2007.

[Westby 2008]

Westby, Jody R. & Power, Richard. *Governance of Enterprise Security Survey: CyLab 2008 Report*. Carnegie Mellon University, 2008.

Copyright © Carnegie Mellon University 2005-2012.

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.

This material has been approved for public release and unlimited distribution except as restricted below.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

DM-0001120