Governing for Enterprise Security: An Implementation Guide

Security Management Conference
November 7, 2007

Julia H. Allen

Organizational Affiliation

Carnegie Mellon University: a private research university in Pittsburgh, PA

Software Engineering Institute: a U.S. federally funded research and development center dedicated to improving the practice of software engineering

CERT Program: transition practices that enable informed trust and confidence in using information technology, to help foster a securely connected world

Governing for Enterprise Security (GES) Implementation Guide

Jody R. Westby, CEO, Global Cyber Risk LLC
Adjunct Distinguished Fellow, Carnegie Mellon CyLab

Julia H. Allen
Carnegie Mellon University, Software Engineering Institute, CERT®

August 2007
TECHNICAL NOTE
CMU/SEI-2007-TN-020

Carnegie Mellon

Why We Wrote This Implementation Guide

Increasing risk exposure & regulatory pressure

Growing market demand for senior executive and board attention

Need for implementable guidance

To define:

- A framework that engages the entire enterprise
- Clear roles, responsibilities & accountabilities
- Actionable steps and outcomes

http://www.cert.org/governance

Deloitte 2007 Global Security Survey

169 financial institutions responding

81% have implemented a formal information security governance framework

- Most of the remaining 19% are in the process

Deloitte 2007 Global Security Survey: The Shifting Security Paradigm. Deloitte, September 2007. http://www.deloitte.com/dtt/cda/doc/content/dtt_gfsi_GlobalSecuritySurvey_20070901(1).pdf

Director of Information Security Governance

Strategic alignment of information security with business strategy

Implement processes to identify, analyze risk; reduce impact to acceptable levels

Measure, monitor, report metrics & security evaluations to senior management

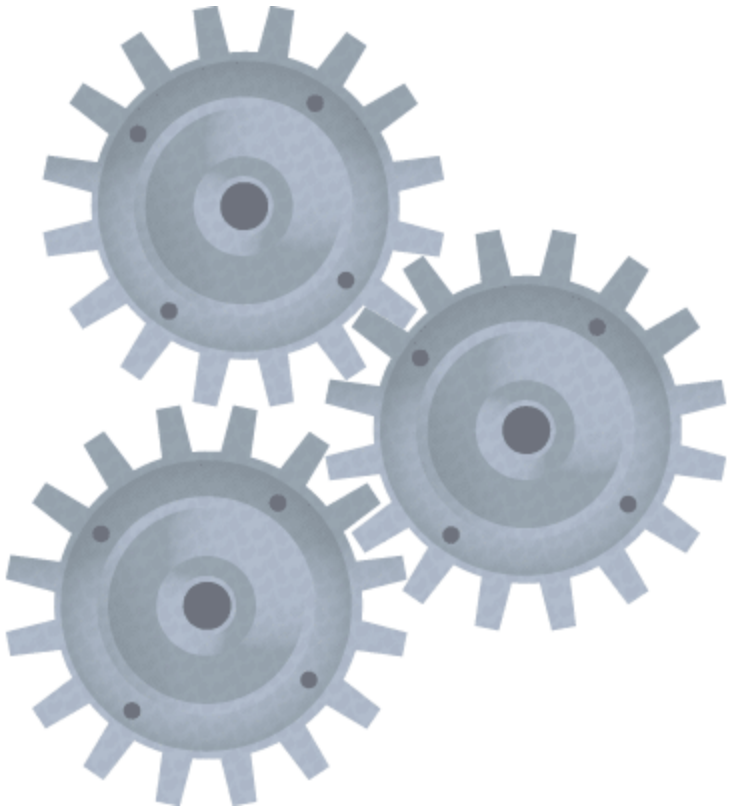
Responsible for business continuity planning, disaster recovery collaboration

American Imaging Management job posting

Governance Defined

Board and executive management responsibilities

- Provide strategic direction
- Ensure objectives are achieved
- Ascertain that risks are managed appropriately
- Verify that resources are used responsibly



International Federation of Accountants. *Enterprise Governance: Getting the Balance Right*, 2004. http://www.ifac.org/Members/DownLoads/EnterpriseGovernance.pdf

Enterprise Governance Actions

- Manage organizational risks & align with strategy
- Protect critical assets
- Make effective use of & preserve resources
- Meet compliance requirements
- Set culture & managerial tone for expected conduct
- Determine strategic direction with goals & policy
- Assure decisions are implemented through effective controls, metrics, enforcement, reviews & audits
- Make governance systemic

Business Roundtable, Principles of Corporate Governance, 2005.

Governing for Enterprise Security

Directing and controlling an organization to establish and sustain a culture of security in the organization's conduct (beliefs, behaviors, capabilities, and actions)

Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business.

Allen, Julia. *Governing for Enterprise Security* (CMU/SEI-TN-023), June 2005. http://www.cert.org/governance.

Information Security Governance

. . . the process of establishing and maintaining a *framework* and supporting *management structure and processes* to provide assurance that information security strategies

- are aligned with and support business objectives
- are consistent with applicable laws and regulations through adherence to policies and internal controls
- provide assignment of responsibility

all in an effort to manage risk.

Bowen, Pauline, et al. *Information Security Handbook: A Guide for Managers* (NIST Special Publication 800-100), October 2006. http://csrc.nist.gov/publications/nistpubs/index.html.

Characteristics of Effective Security Governance

Managed as an enterprise issue

- Horizontally, vertically, cross-functionally

Leaders are accountable

- Visible, own their risks, conduct regular reviews

Viewed as business requirement

- Aligns with objectives, policy, compliance actions

Risk-based

- Compliance, operational, reputational, financial
- Tolerances established and reviewed

Roles & responsibilities defined

- Clear segregation of duties

Characteristics of Effective Security Governance (cont.)

Addressed & enforced in policy

Adequate resources committed

- Includes authority to act, time to maintain competence

Staff aware & trained

- Awareness, motivation, compliance expected

Addressed throughout system development life cycle

- Acquisition -> retirement

Planned, managed, & measured

- Part of strategic, capital, operational planning & review cycles

Reviewed & audited by board committees

- Desired state examined, sustained

Effective vs. Ineffective Governance

On the board's agenda; risk/audit committees actively engaged	Not on the board's radar screen; may get involved after a major incident
Security actions based on a comprehensive risk assessment, established risk tolerances.	Security actions ad hoc
Security managed by a cross-organizational team	Security viewed as a tactical IT concern; business leaders uninvolved
Digital assets inventoried, categorized with assigned owners	No inventory, no assigned ownership, no assessed risk
Security policy actively monitored, enforced; leaders held accountable	Security policy mostly boilerplate; on the shelf
Security program regularly reviewed, audited; subject to continuous improvement	No comprehensive program in place; leaders react when an incident occurs

Challenges & Barriers to Tackle

Ubiquitous access & distributed information

- Supply chains, customers, partners

Enterprise-wide nature of security

- Connection to business mission; distributed roles

Lack of a game plan

- What to do, in what order, how much to invest

Organizational structure & segregation of duties

- Stovepipes, turf issues, conflicts of interest

Complex global legal requirements & risks

Challenges & Barriers to Tackle (cont.)

Assessing security risks & magnitude of harm

- Based on business objectives

Costs & benefits not easily quantifiable

- How much is enough?

Effects of security are often intangible

- Valuing trust, reputation, marketplace confidence

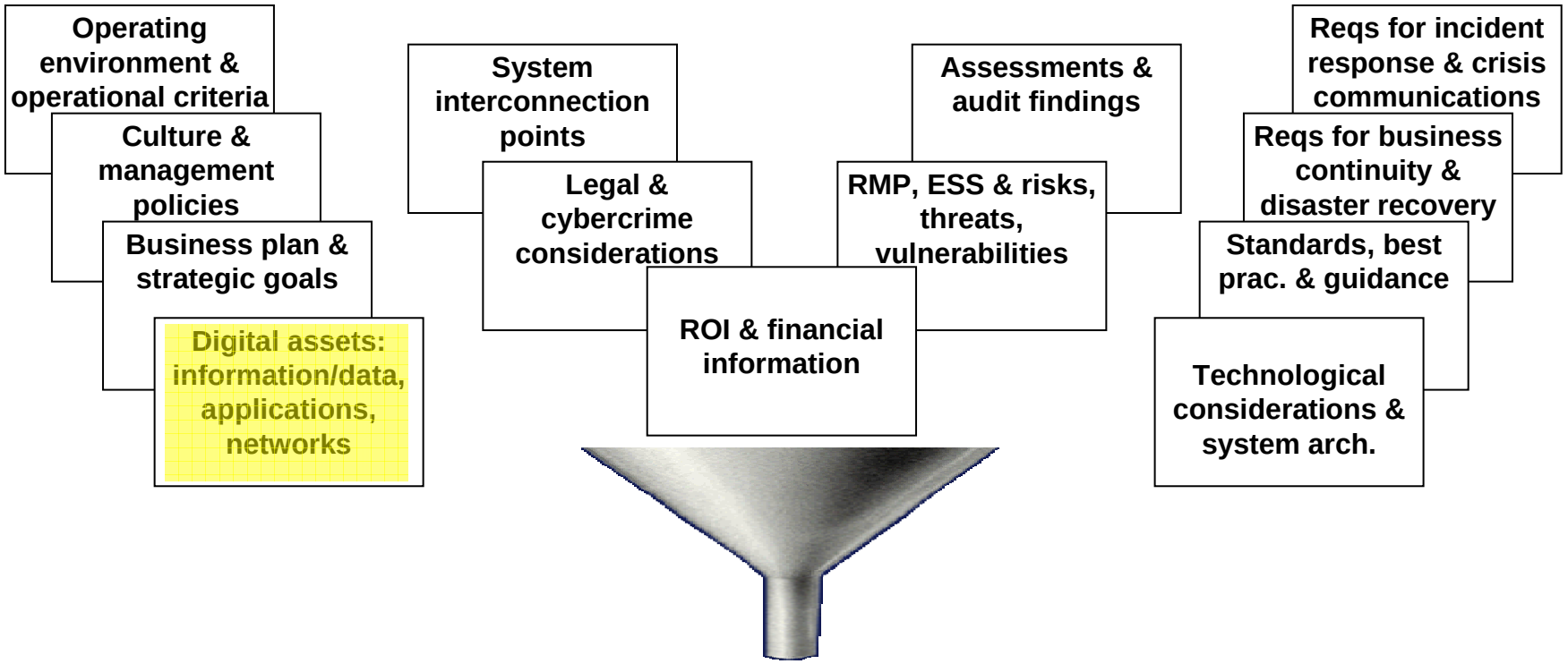
Inconsistent deployment of best practices & measures

Difficult to create & sustain a culture of security

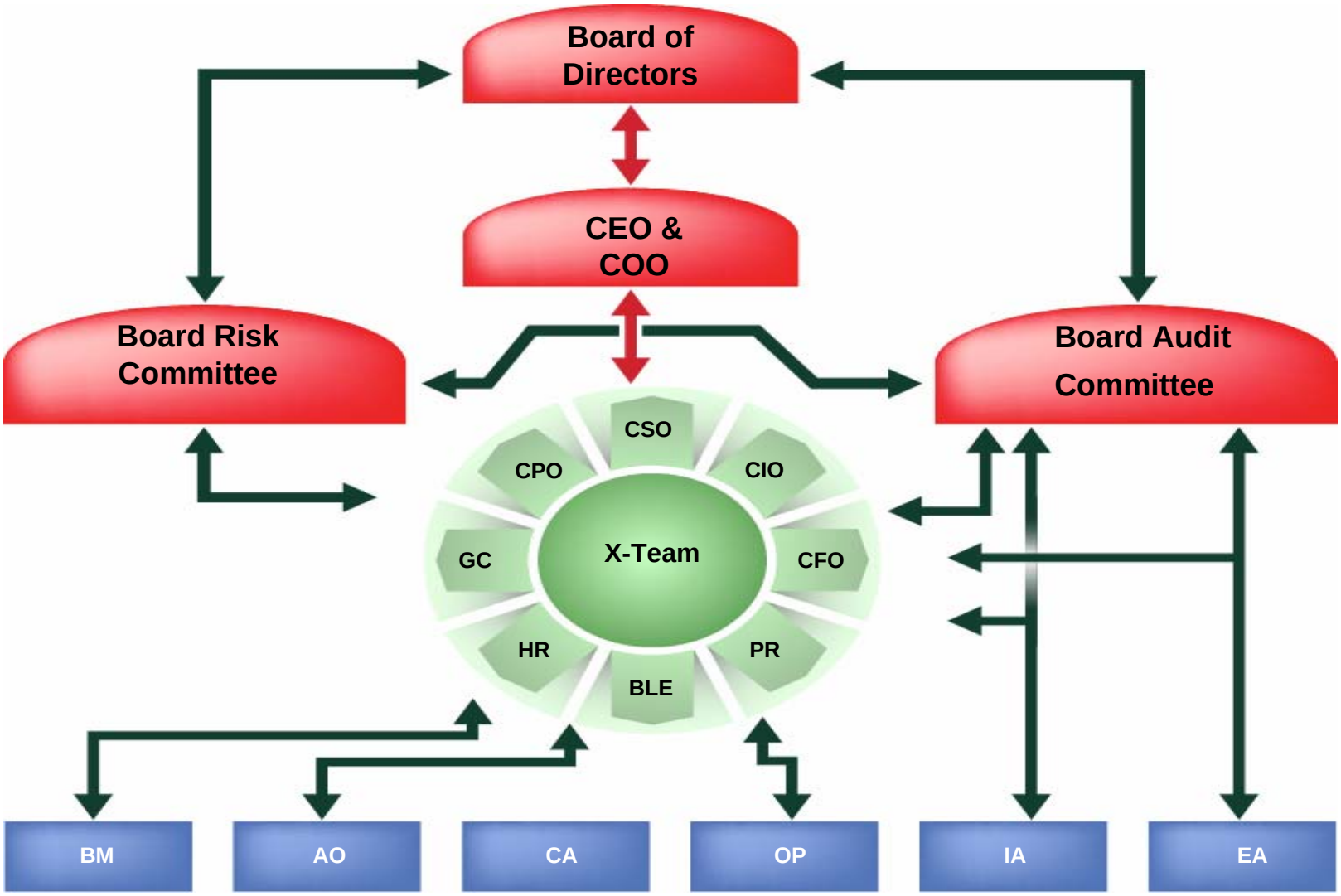
- Leadership & enterprise attention span

Enterprise Security Program (ESP)

Enterprise Security Program Inputs



Governance Structure



ESP Governance Roles

CEO	Chief executive officer
COO	Chief operating officer
CRO	Chief risk officer
C(I)SO	Chief (information) security officer
CIO	Chief information officer
CFO	Chief financial officer
CPO	Chief privacy officer
GC	General counsel
BLE	Business line executives
HR	VP, human resources
PR	VP, public relations

Board Risk Committee

Mission

- Protect shareholder/stakeholder investment
- Protect assets, people, processes, products, reputation from risk

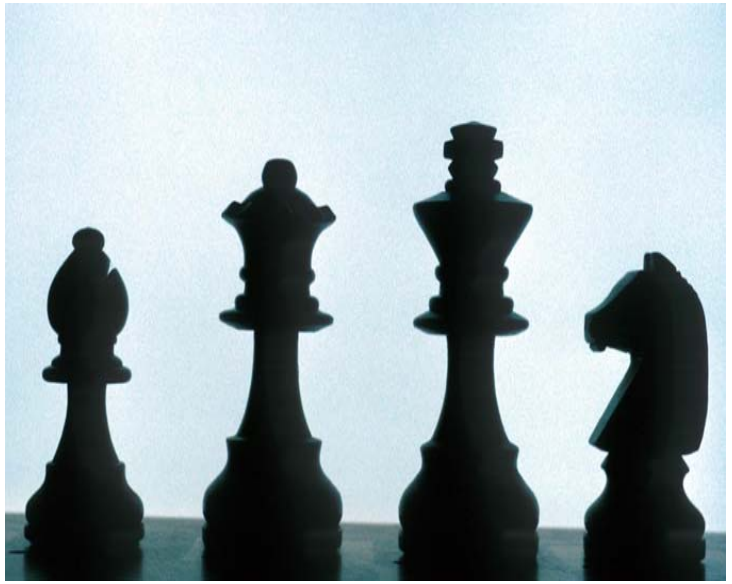
Objectives

- Establish ESP governance structure; allocate responsibilities; oversee ESP
- Set cultural and managerial tone
- Determine risk thresholds/tolerances

Cross-Organizational Team (X-team)

Mission

- Develop and coordinate the ESP
- Coordinate and respond to security risks and incidents



Objectives

- Ensure security risks are addressed
- Ensure that the ESP is integrated with day-to-day business
- Manage the security of digital assets IAW plans and strategies

GES Implementation Guide Framework

Ordered Categories and Activities

- Governance
- Integration & Operations
- Implementation & Evaluation
- Capital Planning & Reviews/Audits

Color Coded Roles

- **Red**: Governance activity; BRC responsibility
- **Green**: X-team responsibility
- **Blue**: Other personnel
- **Purple**: Lead role

Table 2 - ESP Categories, Activities, Responsibilities/Roles, and Artifacts

ENTERPRISE SECURITY PROGRAM*			
CATEGORY	ACTIVITY SEQUENCE	RESP/ROLES	ARTIFACTS
Governance	• Establish Governance Structure • Assign Roles and Responsibilities, indicating Lines of Reporting • Develop Top-Level Policies ↓	BRC	• BRC Mission, Goals, Objectives, & Composition • X-Team Mission, Goals & Objectives, & Members • Organizational Chart • Roles & Responsibilities for ESP • Top-level Policies
	• Inventory Digital Assets • Develop & Update System Descriptions • Establish & Update Ownership and Custody of Assets • Designate Security Responsibilities & Segregation of Duties ↓	CSO, BLE, CIO, BM, AO BLE, CSO, CIO, BM, AO CSO, BLE, CIO, BM, AO BRC, CSO	• Inventory of Assets & Systems[22] • System Descriptions • Ownership & Custody Determined by BLE and Entered on Inventory by CSO • Detailed Security Responsibilities

ENTERPRISE SECURITY PROGRAM*			
CATEGORY	ACTIVITY SEQUENCE	RESP/ROLES	ARTIFACTS
Governance (cont'd)	• Determine & Update Compliance Requirements	GC, CPO, CSO, BLE	• Table of Authorities
	• Map Assets to Table of Authorities	GC, CPO, CSO, BLE	• Mapping of Assets & Authorities
	• Map and Analyze Data Flows	CPO, CSO, BM, AO	• Mapping & Analysis of Data Flows
	• Map Cybercrime and Security Breach Notification Laws and Cross-Border Cooperation With Law Enforcement to Data Flows	GC, CSO, CPO, BLE	• Mapping of Cybercrime & Notification Laws & Cross-Border Cooperation
	• Conduct Privacy Impact Assessments and Privacy Audits ↓	CPO, GC, CSO	• Privacy Impact Assessments • Privacy Audit Report
	• Conduct Threat, Vulnerability, and Risk Assessments (including system C&As)	BRC, CSO, BLE, BM, OP CA	• System Risk Assessments • Certification Letter
	• Determine Operational Criteria	BLE, BM	• Operational Criteria
	• Develop & Update Security Inputs to the Risk Management Plan (RMP)	BRC, CSO, CPO, CIO, GC	• Security Inputs to Risk Management Plan
	• Develop & Update Enterprise Security Strategy (ESS) ↓	BRC, CSO, CPO	• Enterprise Security Strategy

ENTERPRISE SECURITY PROGRAM*			
CATEGORY	ACTIVITY SEQUENCE	RESP/ROLES	ARTIFACTS
Integration + Operations	• Categorize Assets by Levels of Risk & Magnitude of Harm	BRC, CSO, BLE, CPO, GC, BM	• Categorization of Assets
	• Determine & Update Necessary Controls	BRC, CSO, CPO, BLE, GC, BM	• Assignment of Controls (by system)
	• Determine & Update Key Performance Indicators & Metrics ↓	BRC, CSO, BLE, CIO, BM, OP	• Key Performance Indicators & Metrics
	• Identify & Update Best Practices & Standards	CSO, CIO, CPO	• Listing of Approved Best Practices & Standards (BP&S) • Report on Implementation of BP&S • Mapping of BP&S to Controls & Metrics
	• Determine Asset-Specific Security Configuration Settings ↓	CSO	• Asset Security Configuration Settings
	• Develop, Update, & Test Incident Response Plan	BRC, CSO, BLE, CIO, GC, PR BRC, CSO CSO	• Incident Response Plan • Incident Response Plan Test Report • Incident Response Reports
	• Develop, Update & Test Crisis Communications Plan	BRC, PR, CSO, CIO, BLE BRC, PR, CSO, CIO, BLE	• Crisis Communications Plan • Crisis Communications Plan Test Report
	↓	PR, CSO, CIO	• Crisis Communication Reports

ENTERPRISE SECURITY PROGRAM*			
CATEGORY	ACTIVITY SEQUENCE	RESP/ROLES	ARTIFACTS
Integration + Operations (cont'd)	• Develop, Update, & Test Business Continuity & Disaster Recovery Plan • Develop, Update & Verify 3rd Party & Vendor Requirements ↓	BRC, CSO, CIO, BLE, BM, OP BRC, CSO, CIO, BLE BRC, CSO, CIO, BLE BRC, CSO	• Business Continuity & Disaster Recovery Plan • Business Continuity & Disaster Recovery Plan Test Report • 3rd Party & Vendor Requirements for BC/DR, IR, CC • 3rd Party & Vendor Requirements Verification Report
	• Develop & Update Change Management Plans ↓	CSO, CIO	• Change Management Plan • Change Management Logs
	• Develop & Update Enterprise Security Plan • BRC Approval of Enterprise Security Plan ↓	BRC, CSO CSO BRC	• Enterprise Security Plan • ESP Update Report • BRC Approval of Enterprise Security Plan
	• Develop & Update Security Policies & Procedures ↓	CSO, CPO, BLE, HR, GC, PR, BM, OP, AO	• Security Policies & Procedures
	• Develop & Update Security System Architecture Plan ↓	CSO, CIO	• Security System Architecture Plan
Implementation + Evaluation	• Develop & Update ESP Implementation & Training Plans • Implement & Train ↓	BRC, CSO, CPO, HR, BLE, PR, CIO, GC, BM, AO, OP CSO, BLE, BM, OP BRC, CSO, BLE CSO, HR	• Implementation Plan & Results • Training Modules • Training Plan & Schedule • Record of Training

ENTERPRISE SECURITY PROGRAM*			
CATEGORY	ACTIVITY SEQUENCE	RESP/ROLES	ARTIFACTS
Implementation + Evaluation (cont'd)	• Monitor & Enforce Policies & Procedures ↓	CSO, GC, HR, CPO, BLE, BM	• Monitoring & Enforcement Reports
	• Test & Evaluate System Controls, Policies, & Procedures (can include C&A) ↓	CSO, BLE, BM, CA	• Testing & Evaluation Report of Controls, Metrics, Policies & Procedures
	• Identify System Weaknesses & Execute Corrective Action Process (POAM) ↓	CSO, CA, BLE, BM	• System POAMs
	• Issue Authority (or Interim Authority) to Operate ↓	BLE	• Accreditation Decision Letter
Capital Planning + Reviews/ Audits	• Determine Security Business Case, ROI, & Funding ↓	BRC, CSO, CFO BRC	• ESP Security Investment Requirements & ROI Analysis • Board Approved Budget
	• Conduct Formal Review of ESP • Conduct Formal Audit of ESP ↓	BRC, CSO, X-Team BAC, IA, EA, X-Team	• Annual ESP Report (by CSO) • Annual ESP Audit Report (by IA & EA)
	↻ Repeat Process at Designated Intervals, Some Activities Ongoing[23]		

Key Questions the Board Should Ask

Have we identified our critical information assets?

Do we conduct periodic risk assessments?

Do our written security plans & policies address these risks?

Have we implemented our security program? Do we monitor it? Do we regularly reassess it?

Have we addressed employee training issues?

Have we addressed third-party information security?

Are we prepared for a security breach?

Do we view security as part of our day-to-day business?

Smedinghoff, Thomas J. “Director Responsibilities for Data Security: Key Questions the Board Should Ask.” NACD Directors Monthly, April 2007.

For More Information

Governing for Enterprise Security

- www.cert.org/governance

CERT Podcast Series: Security for Business Leaders

- www.cert.org/podcast

ABA Privacy & Computer Crime Committee reports

- International Guide to Combating Cybercrime
- International Guide to Privacy
- International Guide to Cyber Security
- Roadmap to an Enterprise Security Program

For More Information

Julia Allen: jha@cert.org

Jody Westby:
westby@globalcyberrisk.com