

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

CERT Program
Unlimited distribution subject to the copyright.

<http://www.sei.cmu.edu>



This work is sponsored by the U.S. Department of Defense.

The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

Copyright 2007 Carnegie Mellon University.

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.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

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

External use. Requests for permission to reproduce this document or prepare derivative works of this document for external and commercial use should be addressed to the SEI Licensing Agent.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (<http://www.sei.cmu.edu/publications/pubweb.html>).

Table of Contents

Table of Contents	i
List of Figures	iii
List of Tables	v
Acknowledgments	vii
Executive Summary	ix
Abstract	xi
1 Governing for Enterprise Security (GES)	1
1.1 Governing for Enterprise Security Definitions	3
1.2 Eleven Characteristics of Effective Security Governance	5
1.3 Effective versus Ineffective Security Governance	7
1.4 Conclusion	14
2 Defining an Effective Enterprise Security Program	15
2.1 Introduction	15
2.2 Roles	19
2.3 Responsibilities	20
2.4 Activities and Artifacts	25
2.5 Conclusion	32
3 Enterprise Security Governance Activities	33
3.1 Governance Approach	33
3.2 Governance Activities	33
3.3 Additional Considerations	58
3.4 Conclusion	60
3.5 Summary	61
Appendix A: Board Risk Committee: Mission, Goals, Objectives, and Composition	63
Appendix B: Cross-Organizational Team (X-Team): Mission, Goals, Objectives, and Composition	67
Appendix C: Roles and Responsibilities for an Enterprise Security Program	69
Author Biographies	81
Podcast Overview	83
Acronyms	85
Glossary	89
References	93

List of Figures

Figure 1: Enterprise Security Program	16
Figure 2: Enterprise Security Program Inputs	17
Figure 3: Roles Involved in an ESP	25

List of Tables

Table 1: Effective versus Ineffective Security Governance	8
Table 2: ESP Categories, Activities, Responsibilities/Roles, and Artifacts	27
Table 3: Categorization of a Medical Claim System	49

Acknowledgments

The individuals named generously donated their time, knowledge, expertise, and experience to provide peer reviews of selected GES Implementation Guide chapters and artifacts. The authors gratefully acknowledge their comments and contributions.

- Matthew Barrett, Senior Computer Scientist, U.S. National Institute of Standards and Technology
- Robert Charette, President, ITABHI Corporation
- Larry Druffel, (former) President and CEO, SCRA; Teknowledge board member
- Daniel C. Hurley, Jr., Director, Critical Infrastructure Protection, National Telecommunications and Information Administration, U.S. Department of Commerce
- Tom Kellermann, Vice President of Security Awareness, Core Security Technologies
- Paul Love, Director of Information Security, The Standard
- Stephen Northcutt, President, The SANS Technology Institute
- Dr. John H. Nugent, Associate Professor and Director of the Center for Information Assurance, Graduate School of Management, University of Dallas
- Ron Ross, Senior Computer Scientist, U.S. National Institute of Standards and Technology
- Ken M. Shaurette, Engagement Manager, Jefferson Wells
- Dan Swanson, President and CEO, Dan Swanson and Associates
- Ken Tyminski, (former) CISO, Prudential

Please note that participation in the review process does not imply any endorsement of or agreement with the chapters and artifacts they reviewed.

Executive Summary

This guide is designed to help business leaders implement an effective program to govern information technology (IT) and information security. Our objective is to help you make well-informed decisions about many important components of GES such as adjusting organizational structure, designating roles and responsibilities, allocating resources (including security investments), managing risks, measuring results, and gauging the adequacy of security audits and reviews. The intent in elevating security to a governance-level concern is to foster attentive, security-conscious leaders who are better positioned to protect an organization's digital assets, its operations, its market position, and its reputation.

Be forewarned - security is a relatively new area of governance for most organizations. It can be complicated for newcomers to IT and information security. Although the U.S. government has encouraged executives to take a more active role, many still do not understand that security requires action at the governance level. Based on organizations' growing dependence on IT and IT-based controls, information and IT security risks increasingly contribute to operational and reputational risk. Leaders must understand the legal, technical, managerial, and operational considerations that converge in an enterprise security program (ESP). Reading short executive summaries will not suffice. As with audit and compliance responsibilities, boards and senior officers need to thoroughly understand effective enterprise security governance and how to bring it about. For instance, beyond comprehending organizational structure, roles, and responsibilities, leaders need to understand the more detailed responsibilities and tasks required to develop and operate a sustainable security program. Tackling GES is complex, and requires learning information and gaining knowledge that is missing in many organizations today.

The GES Implementation Guide provides such guidance by providing a roadmap that describes actions, roles and responsibilities, and documented outcomes that occur at each step in the roadmap. The materials move from a general introduction and overview to a detailed explanation of how to implement a governance-based ESP. They include:

- Chapter 1: "Characteristics of Effective Security Governance"
- Chapter 2: "Defining an Effective Enterprise Security Program"
- Chapter 3: "Enterprise Security Governance Activities"
- Governance artifact descriptions in appendices for the following:
 - Board risk committee mission, goals, and objectives (Appendix A)
 - Cross-functional security team mission, goals, objectives, and members (Appendix B)
 - Roles and responsibilities (Appendix C)

Chapter 1 presents eleven characteristics that answer the question "How would I know effective security governance if I saw it?" It compares and contrasts both effective and ineffective security governance actions and describes ten key challenges that leaders need to anticipate and address.

Chapter 2 defines the components and sequence of activities in an effective ESP. It is important that senior leaders understand the order and results of needed activities. They also should understand the roles and responsibilities of personnel involved in executing these activities. Sample activities include developing top-level policies, creating and maintaining asset inventories, and determining security inputs to the enterprise risk management plan.

Chapter 3 elaborates on the governance-based activities necessary to achieve and sustain an ESP. It describes the roles of the board risk committee and senior management (C-level or equivalent).

These chapters build upon and extend earlier work: *Governing for Enterprise Security* [Allen 05], *Roadmap to an Enterprise Security Program* [Westby 05], and *International Guide to Cyber Security* [Westby 04b]. This guide assumes that leaders are on the path to implementing a governance- and enterprise-based approach to security for their organizations.

Abstract

Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. If an organization's management does not establish and reinforce the business need for effective enterprise security, the organization's desired state of security will not be articulated, achieved, or sustained. To achieve a sustainable capability, organizations must make enterprise security the responsibility of leaders at a governance level, not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance.

This implementation guide builds upon prior publications by providing prescriptive guidance for creating and sustaining an enterprise security governance program. It is geared for senior leaders, including those who serve on boards of directors or the equivalent. Throughout the implementation guide, we describe the elements of an enterprise security program (ESP) and suggest how leaders can oversee, direct, and control it, and thereby exercise appropriate governance.

Elevating security to a governance-level concern fosters attentive, security-conscious leaders who are better positioned to protect an organization's digital assets, operations, market position, and reputation. This document presents a roadmap and practical guidance that will help business leaders implement an effective security governance program.

1 Governing for Enterprise Security (GES)

Senior leadership's fundamental *commitment* to information security is the most important aspect of effectively managing the security risk to an organization's digital assets. This requires internalizing security as an essential mission need, equivalent to core business operational functions.

The responsibility of boards and officers to protect an organization's digital assets is more than a good idea. It flows from both case law regarding the fiduciary duty of care owed by officers and directors to shareholders, and also flows from legal compliance requirements associated with laws, regulations, treaties, and other legal instruments requiring security or "reasonable care" in protecting data.

Legal compliance requirements originate in domestic and international law. Numerous federal and state laws require protections for various types of data, the most commonly known being financial and medical/health information due to the visibility afforded the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) [Westby 04a]. In addition to GLBA and HIPAA, other U.S. regulations require security of information, such as Internal Revenue Service regulations pertaining to electronic tax records and certain Securities and Exchange Commission (SEC) and Food and Drug Administration regulations. Both federal and state electronic transaction laws also require security for the storage of electronic transaction records [Smedinghoff 06].

Other laws impose governance requirements on specific public and private sector systems. Sarbanes-Oxley, for example, requires public companies to implement internal controls to ensure the integrity of financial data. The Federal Information Security Management Act (FISMA) mandates the development and sustainment of an ESP that is consistent with certain National Institute of Standards and Technology (NIST) standards and guidance. FISMA applies to all federal agencies and departments and contractors operating government systems or maintaining, processing, or storing government data [Westby 04a].

Within the past year, several laws have been enacted that focus on the failure to adequately protect data. For example, security breach notification laws impose a compliance requirement on organizations to notify individuals in the event of a breach of their personal information. Compliance is, therefore, dependent upon knowing whether a breach has occurred and the nature of the incident. Some recently enacted state and federal laws are also imposing security requirements on the destruction of data [Smedinghoff 06].

Case law is helping drive governance over information security. Generally, ESP governance activities flow from the fiduciary duty of care owed by board members and officers to

- govern the operations of the organization and protect its critical assets
- protect the organization's market share and stock price
- govern the conduct of employees
- protect the reputation of the organization
- ensure compliance requirements are met

The majority of U.S. jurisdictions follow the business judgment rule that the standard of care is that which a reasonably prudent director of a similar corporation would have used. This rule has, in the past, generously protected officers and directors from liability for their decisions.

The 1996 shareholder suit, *Caremark International Inc. Derivative Litigation*, raised the notion that shareholders may have a claim against officers and directors for losses arising from the failure to ensure that the organization's information and reporting systems were providing timely and accurate compliance and business performance information [Westby 04a].

More recent cases have developed that theme a bit more. In early 2005, in *Bell v. Michigan Council*, the Michigan court of appeals affirmed a \$275,000 verdict against a union whose members had their identities stolen after documents containing their personal information were stolen from a union official's home. The court agreed that the union had breached its duty to protect the data under Michigan's Social Security Number Act. In a February 2006 case, however, the court was more reluctant to find such a duty of care. In *Guin v. Brazos Higher Education Service Corp. Inc.*, the court viewed the duty of care owed to personal information under GLBA as less than absolute and as more of a "process." In *Guin*, a student sued after a student loan officer took his laptop home and it was stolen. The laptop contained Guin's sensitive, unencrypted personal information.

The student argued that, pursuant to GLBA, the company had a duty of care to protect his information and had breached this duty because the information was not encrypted. The Michigan district court rejected that argument and ruled that the GLBA does not require any specific security measure, such as encryption; the Act only requires reasonable security measures, which were met by the defendant organization's enterprise security program. The court reasoned that since the company's program followed the ESP approach required by the GLBA Safeguard Rule, it, therefore, had the proper "process" in place and had not breached its duty to protect the information even though it was disclosed [Smedinghoff 06].

The GLBA Safeguard Rule, HIPAA, and Federal Trade Commission (FTC) consent decrees involving privacy and security enforcement actions, all require what has become known as the "FTC 4-Part Program." Essentially, this requires the following:

1. Designating appropriate personnel to oversee the privacy and security program
2. Identifying reasonably foreseeable internal and external risks to availability, confidentiality, and integrity of information
3. Conducting an annual written review by qualified persons
4. Adjusting the program to fit findings from reviews, monitoring, and operational changes

From the international perspective, both the Council of Europe (CoE) Convention¹ on Cybercrime (Cybercrime Convention) and the European Union's (EU) *Council Framework Decision on attacks* against information systems specify administrative, civil, and criminal penalties for cybercrimes that were made possible due to the lack of supervision or control by someone in a senior management position, such as an officer or director [Westby 04a]. The Cybercrime Convention continues to gain signatories and additional ratifications, with the U. S. ratification of the treaty being one of the most recent.

In addition, there are market reasons for governance over the security of digital assets. Years ago, a clear correlation was established between drops in stock price and distributed denial of service attacks on corporate systems [Acuff 00]. The Council on Competitiveness has launched a Resiliency Project to examine an organization's ability to avoid, deter, protect, respond, and adapt to market, technology and operational disruptions. A 2006 white paper notes that "resilience in the face of increasing risk is becoming a linchpin of

¹ <http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm>

profitability, shareholder value and competitiveness” [COC 06b]. The Council links resiliency to security by noting in a recent study on system resilience that “[Financial sector] firms with high security levels are likely to have better bond ratings and lower insurance costs” [COC 06a].

The focus on sustainability and corporate responsibility are also pushing the governance envelope. Two “landscape-altering” trends for boards noted by a senior corporate governance executive include the following:

- Sustainability and corporate social responsibility, formerly relegated to gadflies and social interest groups, will be recognized as key corporate governance responsibilities for which directors should be held accountable.
- Organizations will come to recognize that corporate governance is not just a matter of regulatory compliance and accountability but a strategic means to lower the cost of capital, reduce risk, create value, and strengthen the long-term performance of the corporate enterprise [Wilcox 06].

1.1 GOVERNING FOR ENTERPRISE SECURITY DEFINITIONS

This chapter (and subsequent chapters) builds upon established definitions of enterprise governance and IT governance. It then extends and interprets these to explain governance of enterprise security programs (ESP) that protect digital² assets and business operations.

A well-accepted definition of *enterprise governance* as set forth by the International Federation of Accountants (IFAC) and the Information Systems Audit and Control Association (ISACA) is as follows:

Enterprise governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization’s resources are used responsibly [IFAC 04].

The Business Roundtable has determined that effective enterprise governance includes [BRT 05]:

- setting the culture and managerial tone for the conduct of the entity being governed
- specifying a framework for decision making, accountability, and integrity, including assigned roles and responsibilities and codes of conduct
- determining a clear, strategic direction for the organization with defined goals
- directing, controlling, and strongly influencing the entity to achieve stated expectations
- producing financial statements that accurately present the conditions and results of operations and making timely disclosures
- aligning risk management with strategy and ensuring compliance
- conducting effective due diligence and audits of operations and managerial practices
- assuring that decisions are implemented as intended through effective controls, metrics, and enforcement policies
- making governance systemic throughout the organization

² This guide does not specifically address the security or protection of physical assets such as facilities, equipment, and information in physical form, although many of the guidelines are applicable for these types of assets.

Governance extends to the management of an organization's use of IT. The IT Governance Institute declares that [ITGI 03]:

IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.

Enterprise governance and IT governance increasingly encompass the security of IT systems and information. Members of the American Society for Industrial Security (ASIS), the Information Systems Security Association (ISSA), and ISACA (with Booz Allen Hamilton) examined the convergence of security risks and the business operations. In their report, *Convergence of Enterprise Security Organizations*, they adopt the ASIS description of this convergence [AESRM 05]:

[T]he identification of security risks and interdependencies between business functions and processes within the enterprise and the development of managed business process solutions to address those risks and interdependencies.

Governing for enterprise security is defined as [Allen 05]:

- directing and controlling an organization to establish and sustain a culture of security in the organization's conduct (beliefs, behaviors, capabilities, and actions)
- treating adequate security as a non-negotiable requirement of being in business

In its publication, *Information Security Handbook: A Guide for Managers* [Bowen 06], the U.S. National Institute of Standards and Technology (NIST) expands this definition for *information security governance* as follows:

. . . 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.

Governance and management of security are most effective when they are systemic — woven into the very culture and fabric of organizational behaviors and actions. In this regard, culture is defined as the predominant, shared attitudes, values, goals, behaviors, and practices that characterize the functioning of a group or organization. Culture thereby creates and sustains connections among policies, processes, people, and performance. Effective security should be thought of as an attribute or characteristic of an organization. It becomes evident when everyone proactively carries out their roles and responsibilities, creating a culture of security that displaces ignorance and apathy.

To this end, security must come off the technical sidelines as activities and responsibilities solely relegated to software development and IT departments. Today, boards of directors, senior executives, and managers all must work to establish and reinforce a relentless, ongoing drive toward effective enterprise security. If the responsibility for enterprise security is assigned to roles that lack the authority, accountability, and resources to

implement and enforce it – and which do not have organizational connection points horizontally and vertically throughout the organization – the desired level of security will not be articulated, achieved, or sustained.

Contrary to the popular belief that security is a technical issue, even the best efforts to buy software-based security solutions and build security into developed software and operational systems encounter “considerable resistance because the problem is mostly organizational and cultural, not technical” [Steven 06]. Effective security in today’s interconnected environment requires integrating legal, managerial, operational, and technical considerations.

This shift in perspective elevates security from a standalone, technical concern to an enterprise issue. Because security is now a business problem,³ the organization must activate, coordinate, deploy, and direct many of its core resources and competencies so security risks are managed and aligned with the entity’s strategic goals, operational criteria, compliance requirements, and technical system architecture. To sustain enterprise security, the organization must move toward a security management process that is strategic, systematic, and repeatable, with efficient use of resources and effective, consistent achievement of goals [Caralli 04]. Such a process needs to account for the fact that policies, procedures, and technologies are dynamic.

This chapter describes ways to determine if security is being effectively addressed as a governance concern. It compares and contrasts effective with ineffective practices, and it describes some of the challenges that need to be met to ensure a successful security program.

1.2 ELEVEN CHARACTERISTICS OF EFFECTIVE SECURITY GOVERNANCE

One of the best measures that an organization is addressing security as both a governance and management concern is that leaders regularly promulgate a set of beliefs, behaviors, capabilities, and actions that are consistent with security best practices and standards. These measures aid in building a security-conscious culture. They can be expressed as statements about the organization’s current behavior and condition as follows:

1.2.1 An Enterprise-Wide Issue

Security is managed as an enterprise issue, horizontally, vertically, and cross-functionally throughout the organization. The scope of an Enterprise Security Program (ESP) as described here includes people, products, plants, processes, policies, procedures, systems, technologies, networks, and information (P6STNI) [Westby 05].

1.2.2 Leaders are Accountable

Executive leaders understand their accountability and responsibility with respect to security for the organization, for their stakeholders, for the communities they serve (including the internet community), and for the protection of critical national infrastructures as well as economic and national security interests.

Senior leaders visibly engage in the management and oversight of the enterprise security program and support this work with adequate financial resources, effective management, risk-based policies, and annual reviews and audits. Business executives accept responsibility and ownership for the security risks associated with their digital assets (systems, networks, applications, information).

³ See also “Governing for Enterprise Security” [Allen 05] and “Security Is Not Just a Technical Issue” [Allen 06b].

1.2.3 Viewed as a Business Requirement

Security is viewed as a business requirement that directly aligns with strategic goals, enterprise objectives, risk management plans, compliance requirements, and top-level policies. Managers across the enterprise understand how security serves as a business enabler. “Implementation of an effective security program is ultimately a matter of enlightened organizational self-interest” [BSA 03].

Security is considered as a cost of doing business and an investment rather than an expense or a discretionary budget-line item. Security policy is set at the top of the organization and business units and staff are not allowed to decide unilaterally how much security they want.\

This said, appropriate policy exception processes allow the business to continue, while ensuring that leaders have adequate oversight. Adequate and sustained funding and allocation of adequate security resources are a given.

1.2.4 Risk-Based

Determining how much security is enough is based upon the risk exposure an organization is willing to tolerate, including compliance and liability risks, operational disruptions, reputational harm, and financial loss.

Exposure to reasonably foreseeable internal and external risks is examined and tolerance⁴ levels are reset if necessary, as part of the normal process of reviewing organizational performance and risks.

1.2.5 Roles, Responsibilities, and Segregation of Duties Defined

Qualified personnel are assigned to leadership positions – Chief Information Officer (CIO), Chief Information Security Officer (CISO) and/or Chief Security Officer (CSO),⁵ Chief Risk Officer (CRO), and Chief Privacy Officer (CPO). Security roles and responsibilities for business leaders are denoted by separate lines of reporting and a clear delineation of responsibilities that take into account segregation of duties, accountability, and risk management.

1.2.6 Addressed and Enforced in Policy

Security requirements are implemented through well-articulated policies and procedures which are supported by people, procedural, and technical solutions including controls, training, monitoring, and enforcement. Rewards, recognition, and consequences with respect to security policy compliance are consistently applied and reinforced.

⁴ Risk thresholds (and thus risk tolerance) are dependent on organizational context. Several sources suggest establishing these based on how tolerable the impact is if the risk is realized or cost/benefit analysis comparing the cost of mitigation to the benefit of mitigation. Where impacts cannot be tolerated disclosure of customer information, for example), the threshold or tolerance is low and mitigation is required regardless of cost. Where mitigation costs exceed impact, a risk may be deemed acceptable, and then monitored.

⁵ Some organizations have both a CSO and chief information security officer (CISO), with a separation of duties between facilities and personnel security, as well as between information security and information technology (IT) security. As organizations realize, however, that the security of their physical facilities, processes, and personnel is impacted by IT systems and devices, and vice versa, they are integrating the CISO and CSO responsibilities into either a consolidated CSO position or into the chief risk officer (CRO) role [ITCI 06]. As used here, the term CSO encompasses the CISO, although both roles could be subsumed by the CRO. Alternatively, if an organization has both a CSO and CRO, they both participate in the development and sustainment of the ESP, with the CSO taking the lead in implementing the security requirements of the risk management plan, with oversight by the CRO.

1.2.7 Adequate Resources Committed

Key personnel, including IT and security staff, have adequate resources, authority, and time to build and maintain core competencies in enterprise security. This includes the use of security experts, the deployment of technologies, and ongoing education regarding threats, vulnerabilities, and risks to business continuity.

1.2.8 Staff Aware and Trained

All personnel who have access to digital assets understand their daily responsibilities to protect and preserve the organization's security posture. Awareness, motivation, and compliance are the accepted, expected cultural norm. Security awareness and targeted training are conducted routinely and consistently, and security responsibilities are reflected in job descriptions.

1.2.9 A Development Life Cycle Requirement

Security requirements are addressed throughout all system/software development life cycle phases including acquisition, initiation, requirements engineering, system architecture and design, development, testing, operations, maintenance, and retirement.

1.2.10 Planned, Managed, Measurable, and Measured

Security is considered an integral part of normal strategic, capital, and operational planning cycles. Security has achievable, measurable objectives that are integrated into strategic and operational plans, and implemented with effective controls and metrics. Reviews and audits of plans identify security weaknesses and deficiencies, requirements for the continuity of operations, and measure progress against plans of action and milestones (POAMs).

Senior leaders measure this work against defined performance parameters. Managers view security as one of their responsibilities and understand that their team's performance with respect to security is measured as part of their overall performance.

Security is actively considered as part of any new project initiation, acquisition, or relationship, and as part of ongoing project management.

1.2.11 Reviewed and Audited

The board risk and audit committees conduct regular reviews and audits of the ESP. They ensure that all components of the program are maintained and that the ESP continues to sustain the desired state of security for the organization.

1.3 EFFECTIVE VERSUS INEFFECTIVE SECURITY GOVERNANCE⁶

Comparing and contrasting a set of behaviors and actions is useful to further illustrate effective versus ineffective security governance. Sometimes the absence of a quality, value, or cultural norm is a more revealing indicator than its presence. Table 1 presents such a comparison from different perspectives within an enterprise.

⁶ This builds upon and modifies a similar presentation found in an article by Harris [Harris 06].

Table 1: Effective versus Ineffective Security Governance

Effective	Ineffective or Absent
Board members understand that information security is critical to the organization and demand to be updated quarterly on security performance and breaches.	Board members do not understand that information security is in their realm of responsibility, and focus solely on corporate governance and profits.
The board establishes a board risk committee (BRC) that understands security's role in achieving compliance with applicable laws and regulations, and in mitigating organization risk.	Security is addressed ad hoc, if at all.
The BRC conducts regular reviews of the ESP.	Reviews are conducted following a major incident, if at all.
The board's audit committee (BAC) ensures that annual internal and external audits of the security program are conducted and reported.	The BAC defers to internal and external auditors on the need for reviews. There is no audit plan to guide this selection.
<p>The BRC and executive management team set an acceptable risk level. This is based on comprehensive and periodic risk assessments that take into account reasonably foreseeable internal and external security risks and magnitude of harm.</p> <p>The resulting risk management plan is aligned with the entity's strategic goals, forming the basis for the company's security policies and program.</p>	<p>The CISO locates boilerplate security policies, inserts the organization's name, and has the CEO sign them.</p> <p>If a documented security plan exists, it does not map to the organization's risk management or strategic plan, and does not capture security requirements for systems and other digital assets.</p>
A cross-organizational security team comprised of senior management, general counsel, CFO, CIO, CSO and/or CRO, CPO, HR, internal communication/public relations, and procurement personnel meet regularly to discuss the effectiveness of the security program, new issues, and to coordinate the resolution of problems.	<p>CEO, CFO, general counsel, HR, procurement personnel, and business unit managers view information security as the responsibility of the CIO, CISO, and IT department and do not get involved.</p> <p>The CSO handles physical and personnel security and rarely interacts with the CISO.</p> <p>The general counsel rarely communicates particular compliance requirements or contractual security provisions to managers and technical staff, or communicates on an ad-hoc basis.</p>
<p>The CSO/CRO reports to the COO or CEO of the organization with a clear delineation of responsibilities and rights separate from the CIO.</p> <p>Operational policies and procedures enforce segregation of duties (SOD) and provide checks and balances and audit trails against abuses.</p>	<p>The CISO reports to the CIO. The CISO is responsible for all activities associated with system and information ownership.</p> <p>The CRO does not interact with the CISO or consider security to be a key risk for the organization. (See also footnote 5.)</p>
<p>Risks (including security) inherent at critical steps and decision points throughout business processes are documented and regularly reviewed.</p> <p>Executive management holds business leaders responsible for carrying out risk management activities (including security) for their specific business units.</p> <p>Business leaders accept the risks for their systems and authorize or deny their operation.</p>	<p>All security activity takes place within the security department, thus security works within a silo and is not integrated throughout the organization.</p> <p>Business leaders are not aware of the risks associated with their systems or take no responsibility for their security.</p>
Critical systems and digital assets are documented and have designated owners and defined security requirements.	Systems and digital assets are not documented and not analyzed for potential security risks that can affect operations, productivity, and profitability. System and asset ownership are

Effective	Ineffective or Absent
	not clearly established.
<p>There are documented policies and procedures for change management at both the operational and technical levels, with appropriate segregation of duties.</p> <p>There is zero tolerance⁷ for unauthorized changes with identified consequences if these are intentional.</p>	<p>The change management process is absent or ineffective. It is not documented or controlled.</p> <p>The CIO (instead of the CISO) ensures that all necessary changes are made to security controls. In effect, SOD is absent.</p>
<p>Employees are held accountable for complying with security policies and procedures. This includes reporting any malicious security breaches, intentional compromises, or suspected internal violations of policies and procedures.</p>	<p>Policies and procedures are developed but no enforcement or accountability practices are envisioned or deployed. Monitoring of employees and checks on controls are not routinely performed.</p>
<p>The ESP implements sound, proven security practices and standards necessary to support business operations.</p>	<p>No or minimal security standards and sound practices are implemented. Using these is not viewed as a business imperative.</p>
<p>Security products, tools, managed services, and consultants are purchased and deployed in a consistent and informed manner, using an established, documented process.</p> <p>They are periodically reviewed to ensure they continue to meet security requirements and are cost effective.</p>	<p>Security products, tools, managed services, and consultants are purchased and deployed without any real research or performance metrics to be able to determine their ROI or effectiveness.</p> <p>The organization has a false sense of security because it is using products, tools, managed services, and consultants.</p>
<p>The organization reviews its enterprise security program, security processes, and security's role in business processes.</p> <p>The goal of the ESP is continuous improvement.</p>	<p>The organization does not have an enterprise security program and does not analyze its security processes for improvement.</p> <p>The organization addresses security in an ad-hoc fashion, responding to the latest threat or attack, often repeating the same mistakes.</p>
<p>Independent audits are conducted by the BAC. Independent reviews are conducted by the BRC. Results are discussed with leaders and the Board. Corrective actions are taken in a timely manner, and reviewed.</p>	<p>Audits and reviews are conducted after major security incidents, if at all.</p>

Launching an enterprise security program and taking the governance actions necessary to sustain it requires tenacity and perseverance. Organizations may expect to encounter significant challenges along the way. Due to the enterprise nature of these programs, these challenges may occur at all levels of the organization and throughout all phases of the ESP. Understanding them and anticipating how to respond greatly facilitates the process as well as the effectiveness of the ESP.

The good news is that challenges, once mastered, can become opportunities. Leaders who effectively address these challenges can create business opportunities by capitalizing on successful solutions and creating a trusted environment for customers, business partners, and employees.

Challenges to consider often include

- understanding the implications of ubiquitous access and distributed information

⁷ Zero tolerance means that systems are regularly monitored for unauthorized changes. If discovered, such changes are immediately investigated or backed out of operational configurations and a post mortem review is performed to ensure this does not recur. Refer to "Prioritizing IT Controls for Effective, Measurable Security" [Kim 06].

- appreciating the enterprise-wide nature of the security problem
- overcoming the lack of a game plan
- establishing the proper organizational structure and segregation of duties
- understanding complex global legal compliance requirements and liability risks
- assessing security risks and the magnitude of harm to the organization
- determining and justifying appropriate levels of resources and investment
- dealing with the intangible nature of security
- reconciling inconsistent deployment of security best practices and standards
- overcoming difficulties in creating and sustaining a security-aware culture

1.3.1 Ubiquitous Access, Distributed Information

Many boards and executives do not understand the globally connected nature of the internet and how this facilitates access to information distributed throughout an organization and its partner and customer base. Risks and opportunities increasingly derive from who you are connected to (your systems and networks) and who is connected to you.

Robert Metcalfe, the “father of the Ethernet,” has postulated that the value of the network increases at a square of the number of nodes on the net. It is likely that risk increases at an even higher exponent in the world we have today with the internet, where one may essentially reach all. Borders, assuming they exist at all, have been greatly extended whether intended or not.

Today’s marketplace is driven by consumers who have ready and direct access to whomever they wish to transact business with around the world, and who have the option to change their choices with great ease for any reason. Sometimes the needs and requirements of the customer base are different from – or possibly even at odds with – the identified or stated needs and requirements of the business. This creates conflicts and security risks that are important to understand and mitigate.

For example, the need to protect access to sensitive information using strong and multiple layers of authentication and access controls is a business requirement. The need to provide easy and fast access to such information to transact business may be a customer, partner, or supplier requirement.

The tension between business and customer requirements is often reconciled under the presumption that both sides have gone through the process of identifying sensitive information and categorizing it according to a classification scheme to reach an accommodation in terms of levels of protection. Unfortunately, this is often not the case.

1.3.2 Enterprise-Wide Nature of Security

Security must support and protect business processes. Understanding the full breadth and reach of security requires education. Those responsible for security often find that it can be difficult to persuade senior leaders of the need to implement enterprise security in a systemic way. For most organizations and people, security, like insurance, can be an abstract concept, concerned with hypothetical events that may never occur.

Security responsibilities are distributed throughout an organization, requiring cross-organizational interaction, cooperation, and execution. It cannot be contained or delegated to a specific function or department within an

organization or treated as solely a technical problem. Without a clear understanding of enterprise security, the people and processes that play an essential role may be easily missed. Many functions and departments within the organization need to interact to create and sustain an effective security solution that includes strategic, legal, technological, organizational, economic, and social considerations [Westby 05].

At the technical level, this includes making sure security is adequately addressed through the entire system development lifecycle, including phases involving requirements, design, and development or acquisition of software-based systems, rather than waiting until the system is deployed [Bowen 06].

1.3.3 Lack of a Game Plan

Leaders often do not know where or how to start. They lack a framework for action – how to set priorities, assign tasks, get started, and monitor implementation. There are now internationally-accepted approaches to enterprise security that can help organizations determine what should be done and who should do it. There is guidance, such as that offered within this series of chapters, that can help boards and executives better understand how to approach enterprise security. Without such an approach, leaders are unclear regarding how to assign responsibilities, allocate security funding, determine return on investment, and measure performance [BSA 03, Westby 04b].

1.3.4 Organizational Structure and Segregation of Duties

Leaders have often allocated security responsibilities in an ad hoc manner, with many erroneously placing it within the realm of the chief information officer (CIO). If a chief information security officer (CISO) is appointed, often that role reports to the CIO, violating segregation of duties (SOD) principles. The CIO and CISO often have conflicting demands with regard to IT functionality and costs, and they may not be in a position to leverage the resources and authority necessary to address security issues across multiple business lines or divisions. Because little attention is usually given to this issue at the CEO or board level, information security efforts are frequently undercut by the wrong organizational structure [BSA 03, CGTF 04].

Given the close alignment of operational IT and operational security concerns, some organizations may initially have the CISO reporting to the CIO. In this case, however, segregation of duties needs to be explicitly addressed to avoid conflicts of interest. This includes the possible allocation of resources to IT operational activities at the expense of security needs, and sending a message that security is not a high priority resulting in a weakened culture of security.

1.3.5 Complex Global Legal Framework

Enterprise security requirements can flow from a wide range of international, national, state, and local laws and regulations, as well as international standards, policies, and legal contracts. Increasingly, privacy and security requirements around the globe are conflicting or, at best, create multiple layers of differing requirements [Smedinghoff 06, Westby 04a]. “Organizations may be faced with the challenge of implementing different compliance measures” and having to monitor these measures to meet a range of reporting requirements [Bowen 06]. In addition, this regulatory landscape is always changing so security programs need to be reviewed and adjusted on a regular basis to ensure they meet current compliance requirements and keep potential liabilities in check.

Understanding privacy and security requirements is further complicated by the difficulty in accommodating cross-border data flows and meeting compliance requirements of security breach notification and data retention laws. Additionally, vastly differing laws regarding cyber criminal activities create further complexities that must be woven into the ESP [Westby 03].

1.3.6 Understanding Security Risks

Security activities are often under-funded in proportion to the risk and magnitude of the harm that incidents could produce because the security responsibilities are not properly aligned with business operations and risks. Determining the right level of security is a business decision based on the outcomes of an effective risk assessment.

Such an assessment includes an analysis of the foreseeable internal and external risks and the magnitude of harm associated with them. It is important that boards and executives draw on established guidance in assessing risks and understand the harm that could flow to their organization from them [Bowen 06, BSA 03, Stoneburner 02]. When effectively overcome, security risks can also represent opportunities that may preserve and enhance business value and create marketplace advantage.

1.3.7 Cost/Benefit Not Easily Quantifiable

Addressing security at the enterprise level is often hard to justify. Actions taken to secure an organization's assets and processes are typically viewed as disaster-preventing rather than payoff-producing (like insurance), which makes it difficult to determine how best to justify investing in security, and to what level.

The benefits of security investments are often seen only in events that do not happen. As it is impossible to prove a negative, what value does an organization place on cost avoidance?

This difficulty has dogged not only security but also efforts to improve software quality, conduct proper testing, keep documentation up to date, maintain current configuration and hardware/software inventory records, and the like [Braithwaite 02]. Unlike insurance, where the causes of loss are essentially known or change very slowly, the nature of what is considered a security threat and the number and type of vulnerabilities affecting information and systems are constantly evolving and changing.

That said, organizations such as the Congressional Research Service have documented useful guidance and statistics on losses associated with security events [Cashell 04].

They state:

Investigations into the stock price impact of cyber-attacks show that identified target firms suffer losses of one to five percent in the days after an attack. For the average New York Stock Exchange corporation, price drops of these magnitudes translate into shareholder losses of between \$50 million and \$200 million.

1.3.8 The Effects of Security Are Often Intangible

While the tangible effects of a security incident can be measured (in terms of lost productivity and staff time to recover and restore systems), the intangible effects can be an order of magnitude larger. Intangible effects include the impact on an organization's trust relationships, harm to its reputation, and loss of economic and societal confidence resulting from a publicly reported breach.

In terms of its inherent nature, security is sometimes described as an emergent property of networks and the organizations they support. Given security's many dimensions, the precise location where security is enacted cannot be readily identified. An organization's security condition is often determined in the interaction and intersection of people, processes, and technology. As the organization and the underlying network infrastructure change in response to the evolving risk environment, so will the state of an entity's security.

1.3.9 Inconsistent Deployment of Best Practices and Measures

Many organizations do not approach security by deploying sound, commonly accepted practices; rather, they fix problems as they occur and try to keep up with the security risks that accompany change and growth. As a result, establishing an ESP can be an especially daunting task.

Fortunately, there are several widely accepted security best practices and standards. The International Organization for Standardization (ISO) leads the way with ISO 17799 [ISO 05a] and ISO 27001 [ISO 05b]. The National Institute of Standards & Technology has published a series of world-class standards and information security guidance that is applicable to both public and private sector entities.

Professional and technical associations have developed best practices that have been adopted globally by both industry and government. A good example is the Control Objectives for Information and related Technology (CobiT) framework, developed by the Information Systems and Audit Control Association [ITGI 05b].

A growing number of guidelines and checklists, such as those created by the Center for Internet Security, identify practices that are considered acceptable by most professionals [Allen 06d].

Without question, the security situation organizations face today is, in part, due to the lack of attention given these practices and standards. This shortfall is evidenced by the number of vulnerabilities reported to CERT,⁸ many of which have known solutions that have not been implemented. Implementing sound practices and security standards can significantly advance an organization's state of security when properly deployed as part of an ESP. That said, not every practice and standard applies to every organization. Leaders need to ensure that practice selection and implementation directly support business objectives.

1.3.10 Difficulties in Creating and Sustaining a Culture of Security

Achieving a particular state of security is no guarantee that it can be sustained. Security is not a one-time project with a beginning and an end; it is an ongoing process. It requires continuous improvement, monitoring, measuring, and executing (i.e., “doing”) [Allen 06e, ISO 05b]. Continuous improvement requires attention and investment, and security investments often come at the expense of other priorities in terms of accounting and economic opportunity.

Security is hard, often annoying, and something most people and organizations would rather not deal with. There are formidable disincentives to addressing security at more than just a tactical, technical level. As a networked community, there is no perfect solution to effective security, and measures and benchmarks can vary from industry to industry and company to company. This situation is difficult to improve without a significant increase in the reporting of incident cost/loss metrics to estimate probable losses that would have occurred had steps not been taken to reduce risk exposure. Such metrics are analogous to insurance actuarial data, which provides a statistical basis for estimates of loss.

Furthermore, security safeguards are often seen as having negative consequences such as added cost; diminished application, system, and network performance; and user inconvenience (for example, multiple means for authentication that change regularly and are hard to remember). “While internal auditors often identify vulnerabilities within a business system, their recommendations for more stringent system controls are in many cases overruled because of direct costs of implementing and maintaining those controls or because they introduce unwelcome inefficiencies” [Taylor 04]. The board and senior leadership should require formal audits and reviews of the security program, with a formal report card and timely closure of corrective actions.

⁸ CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

Therefore, the board and senior management have a difficult task in setting the tone for security and creating a culture of security awareness with motivation to adhere to security requirements. Policies are not enough; they must be supported with actions from the top that relay the importance of security to corporate operations and competitiveness, and convey the impact that security breaches will have on corporate profits and reputation. This is most effectively done through the development and sustainment of an ESP with active and visible senior leadership involvement [Westby 04b].

1.3.11 Summary

Understanding – and overcoming – challenges facing organizations as they develop and sustain an ESP is part of the process on the path to effective security. Each challenge requires the attention of multiple players within an organization. Thus, challenges can be used as a unifying mechanism through the work of a cross-organizational security team and can help develop buy-in from operational personnel as they contribute to security solutions.

An effective approach to governing and managing enterprise security must confront these challenges head-on, offering counterpoints and benefits to anticipate and offset each challenge. Increasing awareness, knowledge, and understanding of security are necessary first steps toward changing common beliefs. This includes framing the security value proposition to include risk and opportunity.

1.4 CONCLUSION

In today's economic, political, technological, and social environment, addressing security is a core necessity for most, if not all, organizations. Customers are demanding it as concerns about privacy and identity theft rise. Business partners, suppliers, and vendors are requiring it from one another, particularly when providing mutual network and information access. Espionage through the use of networks to gain competitive intelligence and to extort organizations is becoming more prevalent. Domestic and foreign laws and regulations are calling for organizations (and their leaders) to demonstrate due care with respect to security.

An organization's ability to take advantage of new opportunities often depends on its ability to provide open, accessible, available, and secure network connectivity and services. Having a reputation for safeguarding information and the environment within which it resides enhances an organization's ability to preserve and increase market share.

Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. If an organization's management—including boards of directors, senior executives, and all managers—does not establish and reinforce the business need for effective enterprise security, the organization's desired state of security will not be articulated, achieved, or sustained. To achieve a sustainable capability, organizations must make enterprise security the responsibility of leaders at a governance level, not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance.

2 Defining an Effective Enterprise Security Program

2.1 INTRODUCTION

This chapter builds on Chapter 1, “Characteristics of Effective Security Governance” and provides a comprehensive description of an enterprise security program (ESP). It highlights those aspects of an ESP that require governance action. The goal of this chapter is to enable the reader to understand what governance of security means, what it applies to, and how it is exercised.

To be successful, the program requires a security culture and the cooperation of the entire organization. This is achieved by establishing and reinforcing the security “tone” set at the top of the organization, reflected in top-level policies and an effective governance structure. This structure includes a cross-organizational security team, designated key personnel — such as the chief risk officer (CRO), chief security officer (CSO), general counsel (GC), chief information officer (CIO) and others — and the involvement of operational staff. Internal audit has an independent role in auditing the ESP’s effectiveness in addressing organizational security risks.

An ESP consists of a series of activities that support an enterprise risk management plan (RMP) and result in the development and maintenance of

- a long-term enterprise security strategy (ESS)
- an overarching enterprise security plan (which may be supported by underlying business unit security plans and security plans for individual systems)
- security policies, procedures, and other artifacts
- the system architecture and supporting documentation

Figure 1 depicts the hierarchical relationship of these documents and activities.

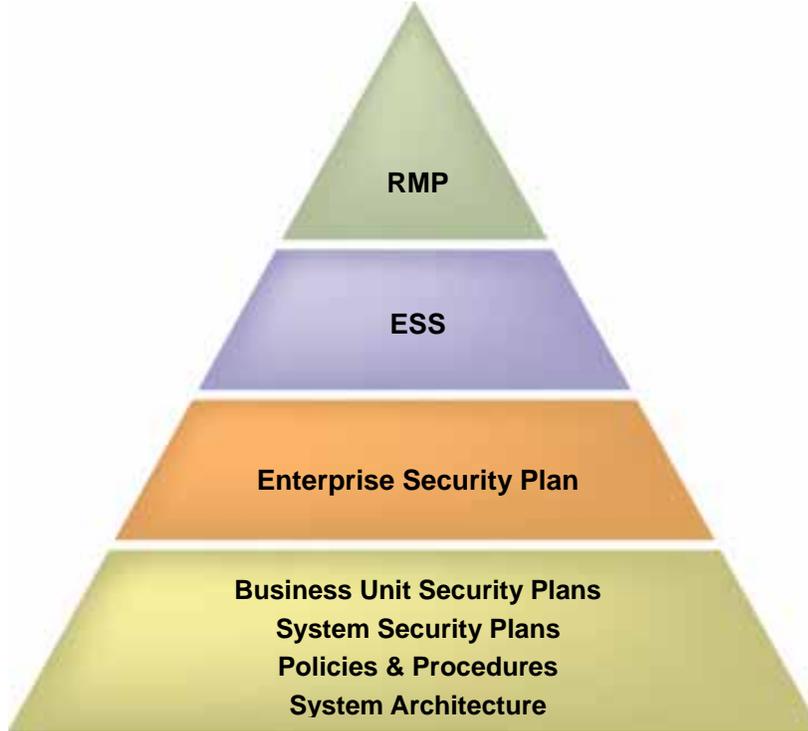


Figure 1: Enterprise Security Program

The development and sustainment of an ESP takes into account a wide array of information, including the organization's RMP, ESS, operational criteria⁹ and culture, top-level policies, compliance requirements, budget, and system architecture.

The RMP reflects the risk decisions of the board of directors risk committee (BRC) or their equivalent, and involves a full consideration of the physical, internal, external, legal, political, cultural, and cyber risks, threats, and vulnerabilities faced by an organization. Figure 2 depicts the various inputs required for an ESP.

⁹ Operational criteria are determined by business line executives (BLEs) and include the baseline IT requirements for the operation of their business unit, such as network availability, interconnectivity requirements, use of portable devices, and number of users requiring software licenses. Operational criteria can also include business continuity and disaster recovery parameters and details regarding the working environment, such as heavy traffic flow within the operational area, physical layout considerations, and extreme climate conditions.

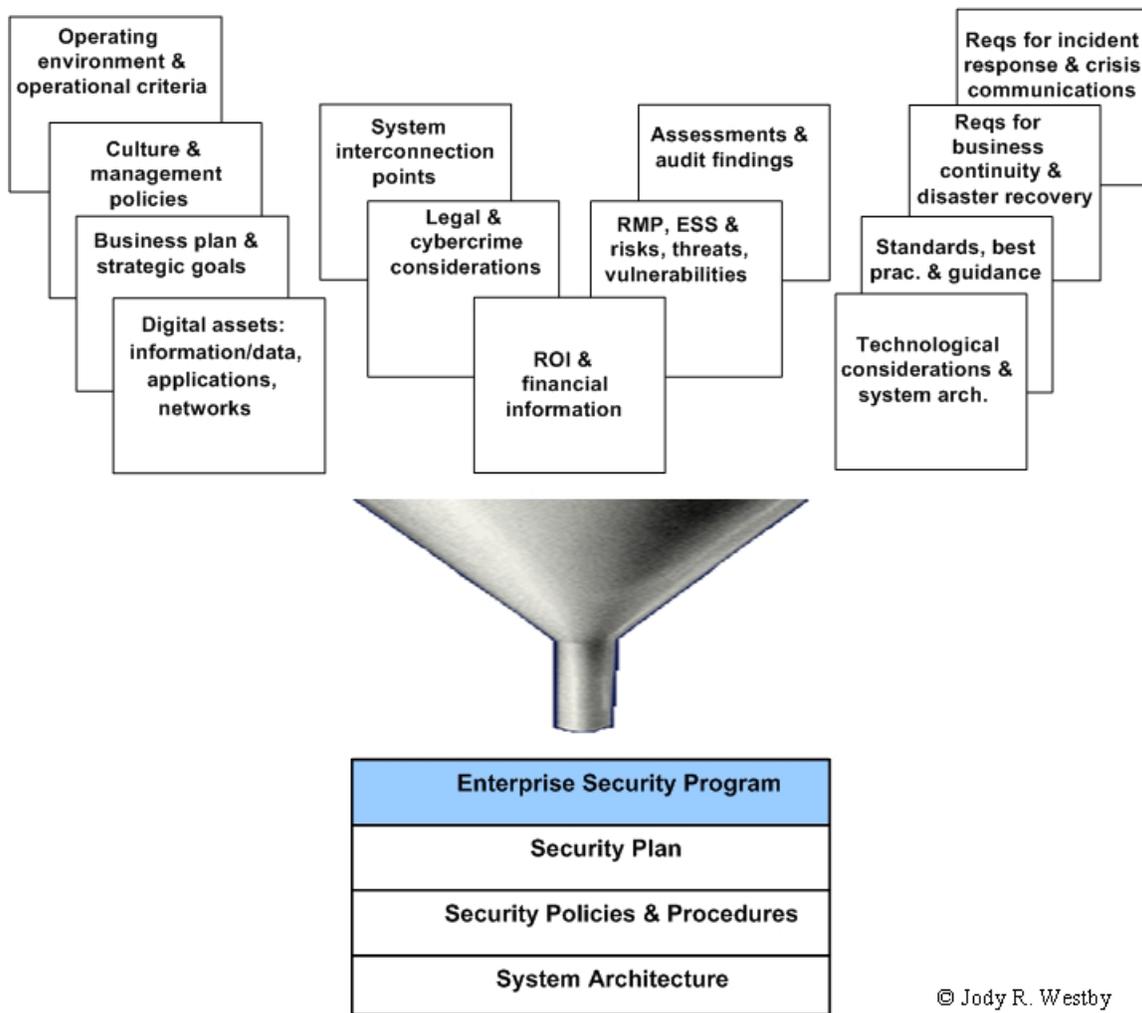


Figure 2: Enterprise Security Program Inputs

The enterprise security plan is the overarching document that serves as the “business plan” for securing an organization’s digital assets,¹⁰ consisting of [Westby 05]

1. information and data
2. applications¹¹
3. networks

The enterprise security plan is developed through a series of activities that produce **artifacts**, or documents, such as asset inventories, risk assessments, categorization of assets, documentation of compliance requirements, plans of action and milestones (POAMs), and various reports.

Security policies are relatively static statements that set the security tone for the entire organization. Policies define the managerial, functional, computing, and security requirements that comprise the program:

¹⁰ As used here, digital assets include information and data, applications, and networks. Systems are groupings of information, applications, and networks. Certifications and accreditations are performed on systems, not individual assets, and it is the system that supports business operations.

¹¹ This includes operating platforms and supervisory control and data acquisition (SCADA) systems.

- Top-level policies are broad statements that support the risk objectives of the RMP that pertain to security. Top-level security governance policies establish the expected behavior and cultural norms that are required to sustain an effective enterprise security program. Topics may include roles and responsibilities, code of conduct, ethics, due care/due diligence, security risk, information protection, and incident response. Top-level security management policies govern operations and the use of technology, such as the use of email and wireless devices; remote access to systems; the protection of intellectual property; business continuity; and critical security controls.
- Functional policies cover operational functions, such as the types of information that require privacy and security protections, who can access this information, and where it may be transmitted or stored.
- Computing policies determine the operating environment and cover topics such as network availability and reliability, backup and recovery requirements (including business continuity), and the like.
- Security policies define the security requirements for the organization's operation, such as authentication controls, encryption, basic authorization limits, incident handling and log requirements, and the like.

Policies are comprised of three parts: the policy content, compliance and monitoring information, and enforcement sanctions.¹²

Security policies are brought to life through **security procedures** that implement policies and required security controls through compliance instructions for everyday operational tasks and responsibilities [Westby 04a]. Different levels in the organization (such as division, department, or business unit) may have unique procedures.

ESP requirements are supported and constrained by the **system architecture**.¹³ For example, network firewalls support the program's security requirements, but a network's interconnectivity with third party networks may constrain the protection of sensitive information and present special security considerations. In this regard, it is important to remember that the system architecture is determined by business requirements, not vice versa. As a general matter, organizations whose business operations are shaped around the technical environment risk losing productivity and competitiveness.

That said, there are instances when the security of the organization as a whole overrides business operational requirements. These business and security trade-offs are resolved by the BRC and senior management, are reflected in the RMP, and are conveyed in top-level policies.

An ESP is comprised of four main categories. Each category represents a sequence of activities (see Table 2) that produce specific outcomes or results (called artifacts) which serve as key inputs to subsequent activities.

The four categories of an ESP are [Westby 05]

1. governance
2. integration and operation

¹² A collection of policies covering a specific topic may have separate compliance, monitoring, and enforcement policies that apply to that topic. For example, all policies requiring encryption may refer to the same compliance, monitoring, and enforcement policies for encryption rather than repeat these provisions in each topic-specific policy.

¹³ System architecture includes the technical network and system components (hardware and firmware), operating platforms and application software, and other hardware or software components used within the IT environment. System architecture differs from "enterprise architecture," which describes the alignment between business functions and IT assets.

3. implementation and evaluation
4. capital planning and reviews/audits

2.2 ROLES

The development of an ESP requires a multidisciplinary approach that engages personnel at all levels throughout the organization. Dr. Ron Ross, senior computer scientist for the U.S. National Institute of Standards and Technology (NIST), notes that

Risk management is not an exact science; rather, it brings together the best collective judgments of the individuals responsible for the strategic planning and day-to-day operations of the business enterprises to provide adequate security for the information systems supporting the ongoing operations and institutional assets of those enterprises. [Ross 06]

The involvement of the appropriate personnel and the proper alignment of roles and responsibilities in each of the four ESP categories are critical to the adequacy and effectiveness of the program.

There are nine groups of personnel involved in the development and sustainment¹⁴ of an ESP:

1. Board risk committee (BRC)
2. Senior officers of the organization: C-level, such as the chief executive officer (CEO), chief operating officer (COO), and chief administrative officer (CAO)
3. Cross-organizational ESP team (X-Team) comprised of
 - general counsel (GC)
 - chief information officer (CIO)¹⁵
 - chief security officer (CSO) and/or chief risk officer (CRO)
 - chief privacy officer (CPO)
 - chief financial officer (CFO)
 - business line executives (BLEs)
 - communications executives (may also include investor relations) (PR)
 - director of human resources (HR)
4. Asset owners (AO)
5. Business managers (BM)
6. Operational personnel, including procurement personnel (OP)
7. Certification agent (CA)
8. Board audit committee (BAC)
9. Internal and external audit personnel (IA, EA)

It is important that each of these groups understand (a) their roles and responsibilities in the development of the ESP and (b) that the multidisciplinary nature of the program requires dovetailing managerial, operational, legal, and technical considerations [Westby 05].

¹⁴ ESPs must be sustained, not merely maintained. They must keep pace with organizational, technical, legal, and operational changes and new requirements, and function as the platform for all security actions and decisions within an organization.

¹⁵ Some organizations have a separate telecommunications officer responsible for networks. This person should also be on the X-Team.

2.3 RESPONSIBILITIES

The clear delineation of roles and responsibilities facilitates X-Team activities and ensures effective governance and accountability. Careful consideration must be given to the segregation of duties (SOD) for the purpose of preserving independence, providing checkpoints, implementing safeguards against abuse, and enabling trusted change management.

The *International Guide to Cyber Security* [Westby 04a] and the Corporate Governance Task Force report “Information Security Governance: A Call to Action” [CGTF 04] are useful references and provide comprehensive descriptions of security governance responsibilities for board of directors, senior executives, executive team members, and senior managers.

2.3.1 Board Risk Committee

The BRC is comprised of independent and non-independent directors and reports to the organization’s board of directors (or equivalent). It has direct responsibility for

- establishing the ESP governance structure for the organization
- setting the “tone” for risk management (including privacy and security) through top-level policies and actions
- ensuring qualified and capable personnel are hired or engaged for the development and sustainment of the ESP
- defining roles and responsibilities and ensuring SOD
- obtaining board approval for the security budget

In its oversight capacity, the BRC works with senior management and is responsible for

- conducting risk assessments and reviews
- developing, approving, and maintaining the organization’s RMP, ESS, and enterprise security plan
- categorizing assets by levels of risk and harm and approving security controls, key performance indicators, and metrics
- steering the development, testing, and maintenance of plans for business continuity and disaster recovery, incident response, crisis communications, and relationships with vendors and other third parties¹⁶
- allocating sufficient financial resources for the development and sustainment of the program based upon a security business case and return on investment (ROI)
- ensuring the ESP is implemented and personnel are effectively trained according to the implementation and training plan
- conducting periodic (no less than annual) reviews of the ESP
- ensuring material weaknesses in the ESP are rectified and the ESP is up-to-date

The BRC has final acceptance authority of the ESS and ESP, and the RMP, which must also be approved by the full board.

¹⁶ The transference of ESP requirements to third parties and outsource service providers requires careful oversight and governance, lest the BRC’s risk management efforts be diluted or forgotten.

2.3.2 X-Team

The X-Team is responsible for the coordination of security issues and the implementation of the BRC-approved RMP, ESS, and enterprise security plan, usually under the direction of a senior executive, such as the chief operating officer (COO) in large organizations or the chief executive officer (CEO) in small- to medium-sized organizations. Members of the X-Team have individual and/or shared responsibility for certain ESP activities, which are noted in Table 2.

Generally, however, the GC, CSO/CRO, CPO, CIO, and BLEs are the anchor members of the X-Team. They shoulder the greatest responsibility for the ESP, with the CSO taking the lead in its development, implementation, and sustainment.

The **CSO** has direct responsibility for the following:

- **Asset Management**
 - developing and maintaining an inventory of all digital assets (including identifying asset owners and custodians)
 - assigning detailed security responsibilities (including SOD)
- **Assessment**
 - conducting security threat and risk assessments (the CA may also share the lead role if a system certification is being performed)
- **Planning and Strategy**
 - providing security input into the development of the RMP
 - developing and maintaining an enterprise security strategy (ESS)¹⁷ that supports the RMP
 - developing, implementing, and maintaining an enterprise security plan
 - developing and maintaining security policies and procedures
 - developing, testing, and maintaining an incident response (IR) plan
 - developing and maintaining security system architecture plan
 - developing and maintaining an ESP training plan and schedule
 - developing security training modules and maintaining training records
 - integrating security requirements into the capital planning and investment process and determining ROI (shared responsibility with CFO)
- **Controls and Performance Management**
 - determining needed controls, and testing and evaluating their effectiveness
 - ensuring the appropriate security standards and best practices have been implemented and security configuration settings conform to the ESP
 - determining and evaluating security key performance indicators (KPI) and metrics
- **Reviews, Certifications, and Audits**
 - supervising the certification and accreditation (C&A) of all systems and the development of plans of action and milestones (POAMs)¹⁸

¹⁷ The RMP covers all risks to an organization, not just information and IT risks, and is usually assigned to CRO or COO. The CSO is responsible for the security aspects of the RMP and develops that portion of the RMP under the oversight of the BRC.

¹⁸ Security *accreditation* is the official management decision given by a senior officer or BLE to authorize the operation of an information system and to explicitly accept the risk to the organization's operations, assets, or personnel based on the implementation of an agreed-upon set of controls. By accrediting an information system, senior management accepts responsibility for

- ensuring material security weaknesses on POAMs are corrected
- conducting reviews of the ESP, including collecting and analyzing program performance measures
- reporting on the program

The **CSO** and **BLE** share responsibility for both documenting systems descriptions, and for categorizing assets by levels of risk and magnitude of harm.

The **CSO** and **CIO** share responsibility for

- developing, testing, and maintaining change management plans
- developing, testing, and maintaining third party and vendor security requirements (with the CSO responsible for the report), with critical input from the BLE
- maintaining appropriate system logs
- monitoring and enforcing change management plans

The **CSO**, **CIO**, and **BLE** share responsibility for developing, updating and testing the business continuity and disaster recovery (BC/DR) plan.

The **GC**, **CSO/CRO**, and **CPO** are responsible for ensuring that (a) all security-relevant compliance and contractual requirements and liability risks have been identified, a Table of Authorities¹⁹ is developed, and digital assets are mapped to the Table of Authorities, and (b) security and privacy risks are adequately mitigated in accordance with the organization’s RMP, ESS, policies, and code of conduct.

The **CPO** is responsible for mapping and analyzing data flows (see Glossary), preparing and conducting privacy impact assessments, and conducting privacy audits to ensure compliance requirements are being met and policies are effective and enforced.

The **GC** is responsible for mapping cybercrime and security breach notification laws to data flows.²⁰ The GC often takes the lead in investigating breaches or incidents, including gathering and protecting evidence, to ensure that evidentiary considerations are taken into account, communications with law enforcement are coordinated, and liability risks are managed.

the security of the system and is fully accountable for any adverse impacts to the organization if a breach of security occurs. The information and supporting evidence (artifacts) needed for security accreditation are developed during a detailed security review of a system, typically referred to as a security *certification*. The certification process involves testing the effectiveness of system controls. Certification and accreditations (C&As) are mandatory for all federal government systems, including those operated by contractors. POAMs assist in identifying, assessing, prioritizing, and monitoring the progress of corrective actions taken to address system weaknesses. POAMs also help identify performance gaps and are useful in conducting oversight [Ross 04, Bowen 06]. Many private sector entities follow a similar process but may not use the same terminology. NIST has published excellent guidance in the area of C&As and POAMs and information security management which serve as valuable reference materials for public and private sector use [Ross 04, Bowen 06]. Therefore, this chapter uses the C&A and POAM terminology to ensure a common understanding of the task that is required.

¹⁹ A Table of Authorities lists all applicable laws, regulations, directives, contracts, and other legal requirements applicable to the organization’s assets and systems.

²⁰ When data is transmitted from one user to another or from one physical location to another, it is called a data flow, i.e., the data flows from one person or place to another. With respect to location, data could flow from one server to another or from one state or country to another. Such flows of data raise numerous security considerations, such as compliance with different laws from jurisdiction to jurisdiction; the policies and procedures required to ensure that security requirements are passed from one user or location to the next; and the technical software and tools that must follow the data to ensure security is effectively deployed and maintained.

The **CFO** is responsible for (a) ensuring the security budget demonstrates acceptable return on investment (ROI) and is tied to the organization's RMP and ESS (this is a responsibility shared with the CSO), and (b) allocating sufficient financial resources to support and sustain the ESP.

BLEs are responsible for assigning ownership and custody of their assets, determining operational criteria, and ensuring that their systems meet the requirements of the security plan and are certified and accredited, if required. The BLE issues the letter granting authority to operate (ATO) or interim authority to operate (IATO). Best practices require BLEs to accept or deny the risks associated with their systems through their granting or denying authorizations to operate.²¹ This role for the BLE reflects the integration of the ESP throughout the organization and indicates how the system architecture supports business operations. Business executives can no longer insulate themselves from the risks associated with the use of technology to fulfill their operational requirements. The risk that the system brings to the organization, therefore, is borne by the business line. Therein lays the incentive for BLEs to ensure their systems meet compliance requirements, are secure, and have effective controls, policies, and procedures.

HR must ensure that security policies and procedures are implemented throughout the HR process and incorporated in job descriptions. HR has key responsibilities in the implementation of identity management (including user authorization) programs. HR assists in managing insider threats, responding to security incidents, and controlling risks associated with temporary, new, and departing personnel, vendors, contractors, and other third parties.

HR, GC, and CSO share the responsibility for monitoring and enforcing policies and procedures.

PR (which can include investor relations) is responsible for the development, testing, and maintenance of crisis communication plans and provides critical input regarding managing risks associated with BC/DR, and IR plans.

2.3.3 Additional Roles

The **BMs** and **AOs** must ensure that the required security controls, policies, and procedures are implemented and the assets they are responsible for (or own)

- meet the requirements of the security plan throughout the system lifecycle
- have undergone security certification (if required)
- have authority to operate (ATO, IATO) from the responsible business line executive

They must also confirm that operational personnel administering the system are adequately trained and change management procedures are followed and enforced.

OP interact as needed with the X-Team, BMs, and AOs. They

- assist with threat and vulnerability assessments
- assist in the identification of appropriate metrics
- participate in the development of policies and procedures

²¹ The offices of the CIO and CSO are also considered business units, in that they own assets and are responsible for them. CIOs, for example, are often owners of an organization's operating platforms and networks and systems utilized in managing information and IT resources, whereas CSOs own security technologies and systems that support the ESP.

- provide input during the development of BC/DR and IR plans
- assist in planning and developing effective training

The OP involved in these activities can be quite diverse, depending upon the size of the organization, the complexity of the systems and processes, and the security required. For example, OP for a manufacturing plant who are included in the development of an ESP could include administrative personnel handling sensitive data (e.g., personal, financial or medical/health data), control room personnel responsible for the operation of business processes controlled by SCADA systems, staff involved in the development of intellectual property (e.g., collaborative design, software development, or research and development teams), and personnel who receive and process orders. OP also includes procurement personnel who are responsible for purchasing equipment or services which have security risks, such as copiers with internal servers.

The CA is an independent agent who reviews all ESP systems and assesses whether they follow prescribed best practices and standards, have the required artifacts (including ATO or IATO), and meet the requirements of the security plan. Upon completion of the certification process, the CA issues a certification letter stating whether the artifacts are all accounted for and properly completed, and identifies weaknesses and deficiencies.

The BAC, IA, and EA are responsible for auditing the ESP to ensure that the ESP is in alignment with the RMP and ESS. They confirm that all activities are properly executed, artifacts are adequate and accounted for, SOD is enforced, and policies and procedures are complied with.

The players and their interactions in the development and sustainment of an ESP are depicted in Figure 3. Green boxes represent anchor members of the X-team. Black arrows denote interactions between the various groups. Blue boxes are operational personnel that interact as needed or periodically, such as IA (internal audit) and EA (external audit).

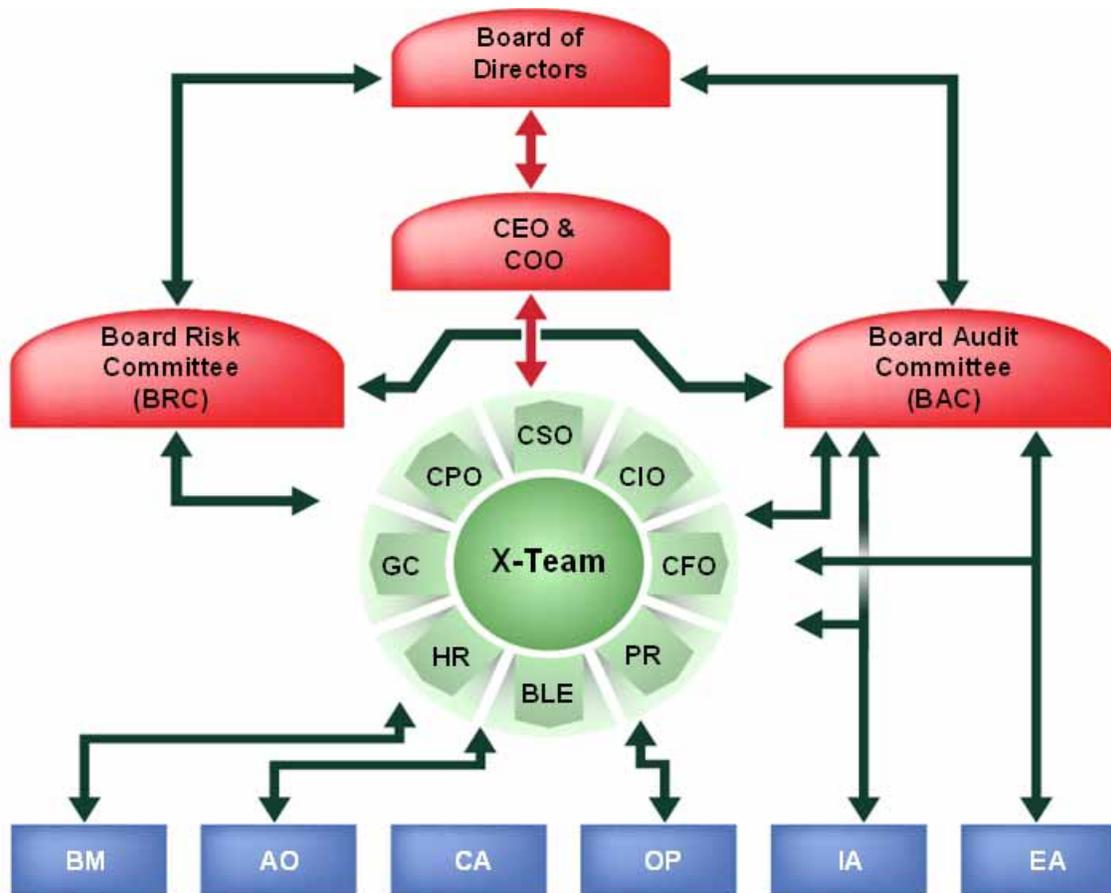


Figure 3: Roles Involved in an ESP

2.4 ACTIVITIES AND ARTIFACTS

Activities and artifacts, in essence, define an ESP. Artifacts are the supporting documents, or outputs, produced by the activities undertaken in the development of an ESP. For example, artifacts produced in establishing a governance structure include

- the mission, goals, and objectives of the BRC and X-Team
- organizational charts depicting lines of reporting
- BRC and X-Team roles and responsibilities
- top-level policies

The sequence of activities undertaken in the development of an ESP is critical. An activity is often dependent upon key artifacts produced by other activities. When activities are undertaken without all of the required inputs from other artifacts, the program may be less effective and the organization may be placed at risk.

For each ESP category, Table 2 defines the sequence of activities, the artifacts produced by each activity, and the roles involved. As a result, the figure is useful in describing the scope of the BRC's oversight responsibilities.

In Table 2, all governance activities are listed in red text, and the roles involved in an activity are color-coded, consistent with Figure 3.

Red: **BRC** responsibility

Green: **X-Team** member responsibility

Blue: **Other personnel** as needed when an activity pertains to their operational responsibilities. For example, AOs and BMs may be involved in mapping cross-border data flows but only for the portion of the activity that applies to the assets they use or own.

Purple: **Lead role**. Lead roles can be performed by one role or the lead role may be a shared responsibility, in which case all of the lead roles are shown in purple. When lead roles are shared, they are usually less effective. Extra controls can help ensure each party fulfills their responsibilities and that shared responsibilities are effectively executed.

Activities that are conducted with oversight from the BRC have the BRC shown in red, with the lead role in purple. Where multiple artifacts are produced from one activity, the roles are noted beside the artifact entry.

Chapter 3, “Enterprise Security Governance Activities,” expands and details the governance activities listed in Table 2.

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

ENTERPRISE SECURITY PROGRAM*			
CATEGORY	ACTIVITY SEQUENCE	RESP/ROLES	ARTIFACTS
Governance	<ul style="list-style-type: none"> • <u>Establish Governance Structure</u> • <u>Assign Roles and Responsibilities, indicating Lines of Reporting</u> • <u>Develop Top-Level Policies</u> <p>↓</p>	BRC	<ul style="list-style-type: none"> • BRC Mission, Goals, Objectives, & Composition • X-Team Mission, Goals & Objectives, & Members • Organizational Chart • Roles & Responsibilities for ESP • Top-level Policies
	<ul style="list-style-type: none"> • <u>Inventory Digital Assets</u> • <u>Develop & Update System Descriptions</u> • <u>Establish & Update Ownership and Custody of Assets</u> • <u>Designate Security Responsibilities & Segregation of Duties</u> <p>↓</p>	<p>CSO, BLE, CIO, BM, AO</p> <p>BLE, CSO, CIO, BM, AO</p> <p>CSO, BLE, CIO, BM, AO</p> <p>BRC, CSO</p>	<ul style="list-style-type: none"> • Inventory of Assets & Systems²² • 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)	<ul style="list-style-type: none"> • <u>Determine & Update Compliance Requirements</u> • <u>Map Assets to Table of Authorities</u> • <u>Map and Analyze Data Flows</u> • <u>Map Cybercrime and Security Breach Notification Laws and Cross-Border Cooperation With Law Enforcement to Data Flows</u> • <u>Conduct Privacy Impact Assessments and Privacy Audits</u> 	<p>GC, CPO, CSO, BLE</p> <p>GC, CPO, CSO, BLE</p> <p>CPO, CSO, BM, AO</p> <p>GC, CSO, CPO, BLE</p>	<ul style="list-style-type: none"> • Table of Authorities • Mapping of Assets & Authorities • Mapping & Analysis of Data Flows • Mapping of Cybercrime & Notification Laws & Cross-Border Cooperation • Privacy Impact Assessments • Privacy Audit Report
	<p>↓</p> <ul style="list-style-type: none"> • <u>Conduct Threat, Vulnerability, and Risk Assessments (including system C&As)</u> • <u>Determine Operational Criteria</u> • <u>Develop & Update Security Inputs to the Risk Management Plan (RMP)</u> • <u>Develop & Update Enterprise Security Strategy (ESS)</u> <p>↓</p>	<p>BRC, CSO, BLE, BM, OP CA</p> <p>BLE, BM</p> <p>BRC, CSO, CPO, CIO, GC</p> <p>BRC, CSO, CPO</p>	<ul style="list-style-type: none"> • System Risk Assessments • Certification Letter • Operational Criteria • Security Inputs to Risk Management Plan • Enterprise Security Strategy

²² NIST defines an information system as “a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information” [Ross 04]. Information resources include networks, applications, and data. C&As are performed on systems, and security requirements apply throughout the system development life cycle (SDLC). A system description includes the purpose of the system, the information resources (or assets) that comprise it, how the assets are used, the asset owners and custodians, any special protections required, etc. [Ross 04].

ENTERPRISE SECURITY PROGRAM*			
CATEGORY	ACTIVITY SEQUENCE	RESP/ROLES	ARTIFACTS
Integration + Operations	<ul style="list-style-type: none"> • <u>Categorize Assets by Levels of Risk & Magnitude of Harm</u> • <u>Determine & Update Necessary Controls</u> • <u>Determine & Update Key Performance Indicators & Metrics</u> 	<p>BRC, CSO, BLE, CPO, GC, BM</p> <p>BRC, CSO, CPO, BLE, GC, BM</p> <p>BRC, CSO, BLE, CIO, BM, OP</p>	<ul style="list-style-type: none"> • Categorization of Assets • Assignment of Controls (by system) • Key Performance Indicators & Metrics
	<ul style="list-style-type: none"> • Identify & Update Best Practices & Standards 	CSO, CIO, CPO	<ul style="list-style-type: none"> • Listing of Approved Best Practices & Standards (BP&S) • Report on Implementation of BP&S • Mapping of BP&S to Controls & Metrics
	<ul style="list-style-type: none"> • Determine Asset-Specific Security Configuration Settings 	CSO	<ul style="list-style-type: none"> • Asset Security Configuration Settings
	<ul style="list-style-type: none"> • <u>Develop, Update, & Test Incident Response Plan</u> • <u>Develop, Update & Test Crisis Communications Plan</u> 	<p>BRC, CSO, BLE, CIO, GC, PR</p> <p>BRC, CSO</p> <p>CSO</p> <p>BRC, PR, CSO, CIO, BLE</p> <p>BRC, PR, CSO, CIO, BLE</p> <p>PR, CSO, CIO</p>	<ul style="list-style-type: none"> • Incident Response Plan • Incident Response Plan Test Report • Incident Response Reports • Crisis Communications Plan • Crisis Communications Plan Test Report • Crisis Communication Reports

ENTERPRISE SECURITY PROGRAM*			
CATEGORY	ACTIVITY SEQUENCE	RESP/ROLES	ARTIFACTS
Integration + Operations (cont'd)	<ul style="list-style-type: none"> • <u>Develop, Update, & Test Business Continuity & Disaster Recovery Plan</u> • <u>Develop, Update & Verify 3rd Party & Vendor Requirements</u> 	<p>BRC, CSO, CIO, BLE, BM, OP</p> <p>BRC, CSO, CIO, BLE</p> <p>BRC, CSO, CIO, BLE</p> <p>BRC, CSO</p>	<ul style="list-style-type: none"> • 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
	↓		
	<ul style="list-style-type: none"> • Develop & Update Change Management Plans 	CSO, CIO	<ul style="list-style-type: none"> • Change Management Plan • Change Management Logs
	↓		
	<ul style="list-style-type: none"> • <u>Develop & Update Enterprise Security Plan</u> • <u>BRC Approval of Enterprise Security Plan</u> 	<p>BRC, CSO</p> <p>CSO</p> <p>BRC</p>	<ul style="list-style-type: none"> • Enterprise Security Plan • ESP Update Report • BRC Approval of Enterprise Security Plan
	↓		
Implementation + Evaluation	<ul style="list-style-type: none"> • Develop & Update Security Policies & Procedures 	CSO, CPO, BLE, HR, GC, PR, BM, OP, AO	<ul style="list-style-type: none"> • Security Policies & Procedures
	↓		
	<ul style="list-style-type: none"> • Develop & Update Security System Architecture Plan 	CSO, CIO	<ul style="list-style-type: none"> • Security System Architecture Plan
	↓		
	<ul style="list-style-type: none"> • <u>Develop & Update ESP Implementation & Training Plans</u> • Implement & Train 	<p>BRC, CSO, CPO, HR, BLE, PR, CIO, GC, BM, AO, OP</p> <p>CSO, BLE, BM, OP</p> <p>BRC, CSO, BLE</p> <p>CSO, HR</p>	<ul style="list-style-type: none"> • Implementation Plan & Results • Training Modules • Training Plan & Schedule • Record of Training

ENTERPRISE SECURITY PROGRAM*			
CATEGORY	ACTIVITY SEQUENCE	RESP/ROLES	ARTIFACTS
Implementation + Evaluation (cont'd)	<ul style="list-style-type: none"> • Monitor & Enforce Policies & Procedures ↓	CSO, GC, HR, CPO, BLE, BM	<ul style="list-style-type: none"> • Monitoring & Enforcement Reports
	<ul style="list-style-type: none"> • Test & Evaluate System Controls, Policies, & Procedures (can include C&A) ↓	CSO, BLE, BM, CA	<ul style="list-style-type: none"> • Testing & Evaluation Report of Controls, Metrics, Policies & Procedures
	<ul style="list-style-type: none"> • Identify System Weaknesses & Execute Corrective Action Process (POAM) ↓	CSO, CA, BLE, BM	<ul style="list-style-type: none"> • System POAMs
	<ul style="list-style-type: none"> • Issue Authority (or Interim Authority) to Operate ↓	BLE	<ul style="list-style-type: none"> • Accreditation Decision Letter
	<ul style="list-style-type: none"> • <u>Determine Security Business Case, ROI, & Funding</u> ↓	BRC, CSO, CFO	<ul style="list-style-type: none"> • ESP Security Investment Requirements & ROI Analysis
	<ul style="list-style-type: none"> • <u>Conduct Formal Review of ESP</u> ↓	BRC	<ul style="list-style-type: none"> • Board Approved Budget
	<ul style="list-style-type: none"> • <u>Conduct Formal Audit of ESP</u> ↓	BRC, CSO, X-Team	<ul style="list-style-type: none"> • Annual ESP Report (by CSO)
Capital Planning + Reviews/ Audits	<ul style="list-style-type: none"> • <u>Conduct Formal Audit of ESP</u> ↓	BAC, IA, EA, X-Team	<ul style="list-style-type: none"> • Annual ESP Audit Report (by IA & EA)
	<ul style="list-style-type: none"> • Repeat Process at Designated Intervals, Some Activities Ongoing²³ 		

*© Jody R. Westby and Carnegie Mellon University, 2007. All rights reserved.

²³ Enterprise Security Programs require regular reviews, audits, and updates. Some activities, such as testing the effectiveness of controls, monitoring and enforcing policies and procedures, and revising compliance requirements are performed on an on-going or periodic basis, as needed. This sequence of activities should be viewed as a continuing cycle, with activities beginning again from the top each time the ESP is reviewed.

2.5 CONCLUSION

The development and sustainment of an ESP is an ongoing effort that requires board involvement and oversight and the participation of personnel both “horizontally” and “vertically” throughout an organization. The ESP process relies on a wide range of inputs and each activity produces critical inputs to other activities in support of an organization’s risk management plan. Activities that are undertaken by the BRC and X-Team, and the artifacts that are produced, are done in a coordinated manner, with leadership and key personnel playing specified roles and carrying out defined responsibilities. The blend of legal, technical, operational, and managerial considerations in these activities help establish resilient operations and manage risks. Careful segregation of duties protects against conflicts and establishes appropriate checks and balances to manage risk. Assessments and audits help ensure that

- the ESP is in alignment with the RMP
- effective controls and metrics are used to measure performance
- appropriate business continuity and disaster recovery, incident response, crisis communications, and change management plans have been developed and tested
- the enterprise security plan has been implemented and personnel are trained
- adequate financial resources are allocated to the RMP

Outsourced activities require oversight to ensure the vendor is supporting the client’s compliance and security requirements. Technological innovations and adjustments to business operations, including the use of new technologies, requires the BRC and CSO to remain vigilant and adjust the ESP as necessary to protect against new security vulnerabilities and threats.

The governance structure is the defining activity that serves as the foundation and sustains all others.

3 Enterprise Security Governance Activities

This chapter elaborates the description of an enterprise security program (ESP) discussed in Chapter 2, “Defining an Effective Enterprise Security Program.” It closely examines the governance elements of an ESP, including who is involved, their roles and responsibilities, governance activities required to implement an ESP, and a description of these activities.

3.1 GOVERNANCE APPROACH

ESP governance activities are driven by the board risk committee (BRC), senior management, and designated key personnel. They are undertaken in a manner consistent with an organization’s risk management and strategic plans, compliance requirements, organizational structure, culture, and management policies. Governance activities facilitate the development, institutionalization, assessment, and improvement of the ESP. The IT Compliance Institute declares:

Everyone in the organization has a role in ensuring a successful ERM [enterprise risk management] program, although management bears the primary responsibility for identifying and managing risk and implementing ERM with a structured, consistent, and coordinated approach. Boards of directors and their non-corporate equivalents have an overarching responsibility for monitoring the risk program efforts and obtaining assurance that the organization’s risks are being acceptably managed [ITCI 06].

Although early efforts to engage boards and officers in information security and infrastructure protection were driven from the audit side of governance, the responsibility for setting the organization’s risk threshold, determining its risk management processes and responses, and implementing ERM measures rests with the BRC [ITCI 06]. For purposes of this chapter, ERM is evidenced through the activities of the BRC, including the development and maintenance of the risk management plan (RMP).

The role of the board risk committee, as noted above, has both direct and oversight responsibilities in the development and sustainment of an ESP. The BRC’s direct responsibilities are all within the Governance category of the ESP. Certain BRC oversight responsibilities, however, pertain to activities performed by key cross-organizational team (X-team) personnel in other categories of the ESP. It is important that organizations make a cognizant effort to avoid “stove piping” ESP activities and remain vigilant that security remains an enterprise issue and activities do not become isolated functions [ISACA 05a].

3.2 GOVERNANCE ACTIVITIES

Governance of enterprise security consists of activities which are performed by the BRC and designated X-team personnel, with support from other staff as needed. Guided by Table 2, (ESP Categories, Activities, Responsibilities/Roles, and Artifacts), this chapter describes which ESP activities require governance action. Governance-based ESP activities are grouped into the Table 2 categories of Governance, Integration and Operations, Implementation and Evaluation, and

Capital Planning and Reviews/Audits and are shown in red text in Table 2. Each section also describes the purpose of the artifacts created during each activity.

3.2.1 Governance Category Activities #1 – Structure and Tone

- Establish Governance Structure
- Assign Roles and Responsibilities, Indicating Lines of Reporting
- Develop Top-Level Policies

3.2.1.1 Establish Governance Structure

The purpose of the governance structure is twofold: to establish the appropriate linkages among the various business units, technical and legal personnel, senior executives, and operational staff in a manner that ensures the requisite transparency and coordination; and to develop inputs needed for effective oversight of activities and risk management.

The BRC establishes and regularly reviews the governance structure for information security and risk management. NIST's Ron Ross [Ross 06] notes:

The most important aspect of effectively managing the risk to the organization's operations and assets associated with operating enterprise information systems is a fundamental commitment to information security on the part of the senior leadership of the organization. This commitment is the internalizing of information security as an essential mission need. . . . Information security requirements must be considered at the same level of importance and criticality as the main stream functional requirements established by the enterprise.

One of the first artifacts produced is the BRC Mission, Goals, Objectives and Composition, which includes board member composition (independent and non-independent) and senior executives designated as liaisons to the BRC. This artifact should be approved by the entire board.

3.2.1.2 Assign Roles and Responsibilities

In determining the appropriate lines of reporting and division of responsibilities, the BRC must consider how the governance structure itself can deter fraudulent or malicious acts or prevent errors and unintended consequences. Segregation of duties (SOD) is one of the most important aspects of the governance structure. Since IT systems control nearly all business functions today, and the interconnected nature of networks enable a vulnerability in one area of an organization to permeate others, SOD for change management and control over the system architecture is particularly important. Across the organization, however, there are other points where overlapping responsibilities can create vulnerabilities and audit issues.

At the highest levels of an organization, sound practices result in the separation of IT management and security responsibilities. One of the most frequent violations of SOD involves the lack of independence of CSO and CIO functions. As a matter of good governance, the CSO should not report to the CIO. When the CSO reports to the CIO, there is an inherent conflict of interest. The CIO controls the budget and security funding can be reduced in favor of other projects that the CIO designates as higher priority. Additionally, the CIO can disallow security measures which may interfere with planned operations or suppress response activities. Although the U.S. Federal

Information Security Management Act (FISMA) has the CISO reporting to the CIO for federal entities, the act has been criticized for these same reasons and efforts are now afoot to seek legislative amendments to enable the CISO to have an independent budget and responsibilities.

The CIO and CSO ideally report to a senior executive, usually the CEO, CRO, or chief operating officer (COO). If an organization has a robust CRO position in place, the CIO and CSO (if the CSO position has not been collapsed into the CRO position) may report to that person. The CRO usually reports directly to the CEO or the COO. The greater the independence accorded to the CRO, the better.

If the CSO reports to the CIO, SOD is absent. Care must be taken to put checks-and-balances, review/audit processes, and other controls in place to guard against abuses and conflicts of interest.

The Corporate Governance Task Force Report, submitted to the U.S. Department of Homeland Security (DHS) in 2004, offers some suggested organizational charts for SOD and CIO, CSO, and CRO lines of reporting [CGTF 04]. At a more detailed level, organizations, such as the Information Systems Audit and Control Association (ISACA), have developed useful materials to guide BRCs and senior management in SOD and establishing the appropriate governance structure [ISACA 05b].

3.2.1.3 Develop Top-level Policies

Top-level policies developed by the BRC and senior executives should be tailored toward SOD and reinforce lines of reporting. They should establish the risk thresholds for the organization, and specify guidelines for mitigating and accepting security risks as well as tolerable levels of residual risk once mitigating actions are in place. These policies are usually high-level, rather static statements that are consistent with the organization's code of conduct and ethics policies. Care should be taken in both drafting and reviewing top-level policies, as they set the security "tone" for the organization and serve as guideposts for more detailed operational risk policies that are determined by senior and mid-level management.

Artifacts: The artifacts produced during these activities include the following:

- BRC Mission, Goals, and Objectives and Composition
- X-team Mission, Goals and Objectives, and Members
- Organizational Chart, indicating lines of reporting
- Roles and Responsibilities
- Top-level Policies

Collectively, they serve to set the tone and direction for security for the entire organization. These documents demonstrate the organization's commitment to security and its expectations. The roles and responsibilities and polices establish clear SOD and accountability.

3.2.2 Governance Category Activities #2 – Assets and Responsibilities

- Inventory Digital Assets
- Develop and Update System Descriptions
- Establish and Update Ownership and Custody of Assets
- Designate Security Responsibilities and Segregation of Duties

3.2.2.1 Inventory Digital Assets

An inventory of digital assets is one of the most essential inputs into the development of an ESP. Inventories are used to

- conduct C&As on systems (comprised of networks, applications, and data)
- determine the categorization levels for the assets and appropriate controls
- aid in the monitoring, testing, and evaluation of information security controls
- identify system weaknesses and develop POAMs
- support information resources management
- assist IT planning, budgeting, and acquisition processes
- facilitate risk management

The inventory consists of separate sections, with inventories for each asset class (networks, applications, and data) as well as an inventory of systems (groupings of networks, applications, and data). System inventories are critical because C&As are performed on systems, not individual assets, and it is the system that supports business operations. Therefore, determination of the system boundary is important.²⁴

A system is identified by constructing logical boundaries around a set of processes, communications, storage, and related resources. The elements within these boundaries constitute a single system requiring a system security plan. Networked systems make the boundaries much harder to define. Many organizations have distributed client-server architectures where servers and workstations communicate through networks, and those same networks are connected to the internet.

Some organizations consider a system to be a composite of people, procedures, materials, tools, equipment, facilities, hardware, and software operating in a specific environment to achieve a specific purpose, support, or mission requirement [Swanson 06, Ross 04]. Such inventories are more technical in nature and can be quite detailed, capturing specifics regarding these data points.

Other organizations take more of a “business process” approach to system inventories, linking the applications that can be grouped by business function, with the associated databases and networks. Systems may contain subsystems. For example, an inventory entry for a financial management system may have accounts payable, accounts receivable, and general ledger

²⁴ System boundaries are determined by the IT resources assigned to a particular system [Swanson 06]. System boundaries are usually determined during the inventory process.

components, and include both required databases and the networks it uses. This could be considered one system, with each component treated as a subsystem.

Other organizations may decide to break the system boundary into smaller components, with each of the accounting functions categorized as a separate system. When a system boundary is too finely subdivided, the C&A and documentation costs can become prohibitive. Likewise, however, if a system boundary encompasses too many applications (subsystems), C&As often have to be repeated for the entire system to accommodate modifications to one or more subsystems.

NIST has developed excellent guidance on determining system boundaries for use by federal entities subject to the Federal Information Security Management Act (FISMA) [Swanson 06, Ross 04]. NIST notes that the process of establishing system boundaries should include all key participants. The guidance is also useful for private sector entities. NIST guidance affords federal agencies considerable leeway in determining what constitutes a system, but it offers the following guidelines for determining system boundaries. Generally, the assets should

- be under the same direct management control
- have the same function or mission objective
- have essentially the same operating characteristics and security needs; and
- reside in the same general operating environment or, if a distributed system, reside in locations with similar operating environments

The inventory should gather key data points, including the interconnection points between each system and other systems or networks, including those not operated by or under the control of the organization.

The CSO takes the lead in the development of the inventory of assets and is assisted as needed by the CIO, BLEs, BM, and AO. As with all artifacts in an ESP, it is important that the inventory be reviewed regularly (at least annually) and updated to ensure its accuracy and sustain its usefulness as a foundation of the ESP. Routine updates to the inventory should be managed through effective change management procedures and documentation.

3.2.2.2 Develop and Update System Descriptions

System descriptions serve as the main repository for information regarding the system, its purpose and how it is used, other key data about the resources it uses, and more. The information will vary depending upon the size and complexity of the system and where it is in its system development lifecycle (SDLC).

Information that is commonly included in a system description includes the system name and purpose, the system owner, organizational unit responsible for the system, the person responsible for security of the system, hardware and software used by the system, network settings, and other physical and security information [Ross 04].

The CSO and BLEs take the lead in the development and maintenance of the system descriptions and are assisted as needed by the CIO, BM, and AO (including system owner).

3.2.2.3 Establish and Update Ownership and Custody of Assets

Determining ownership of assets is critical. This is an activity that is determined by the BLE and entered on the inventory by the CSO. The CIO, BM, and AO assist as needed and provide access to personnel using the systems and assets under their control. Owners serve as the point of contact for the assigned asset, and they are responsible for coordinating activities regarding the asset, including its use in systems.

Owners are also assigned to systems. System owners must have full knowledge of the system, including its capabilities and functionalities and how assets used within a system are handled. The system owner is responsible for all SDLC activities pertaining to the system [Swanson 06].

Owners, however, may not always have custody of their assets. Information used in system A, for example, may be processed and transmitted for processing and storage by system B. In this situation, the designated custodian of the data is a person aligned with system B. The custodian has responsibility for the stored information and is required to follow defined security measures, but does not have ownership responsibilities. Likewise, an application may be “owned” by a particular business unit, with ownership of the application assigned to a manager in that unit. Other units may also use the application but are not necessarily a designated owner or custodian. In this situation, the custodian of the application could be a person on the CIO’s staff responsible for maintaining the application software on the corporate server for use by its users and owner. Ownership and custodianship are entered in the inventory and in the system description.

3.2.2.4 Designate Security Responsibilities and Segregation of Duties

Designating security responsibilities for assets is particularly important in large organizations or for large, distributed systems. SOD at the operational level is equally significant. Absent appropriate SOD and enforced policies and procedures, custodians of data could, inadvertently or intentionally, allow data to be used for unauthorized purposes. Users of applications without ownership authority could authorize modifications to the application if SOD and a rigorous change management process are not in place. These are examples of breakdowns in segregation of duties that can wreak significant havoc and bring substantial risk to an organization [ISACA 05b]. The CSO has lead responsibility for designating detailed security responsibilities and ensuring SOD is in place or, if not, that this is managed through policies, procedures, and checkpoints. The BRC exercises oversight of this activity.

Artifacts: The artifacts produced during these activities include the following:

- Inventory of Assets and Systems (including ownership and custody)
- System Descriptions
- Detailed Security Responsibilities for Assets

3.2.3 Governance Category Activities #3 – Compliance

- Determine and Update Compliance Requirements
- Map Assets to Table of Authorities
- Map and Analyze Data Flows

- Map Cybercrime and Security Breach Notification Laws and Cross-Border Cooperation with Law Enforcement to Data Flows
- Conduct Privacy Impact Assessments and Privacy Audits

3.2.3.1 Determine and Update Compliance Requirements

Managing legal compliance and risk considerations is very tricky in today's business environment. This task is a shared responsibility of the GC, CPO, and CSO. They may be assisted by the BLEs as needed. Global operations require the transmission of an extensive amount of data across borders to transact business. Such cross-border data flows create significant risks because the global, legal framework for privacy and security requirements is highly complex and inconsistent.

Cross-border data flows resulting from outsourcing and globalization of operations are complicating the development and sustainment of ESPs even further. Therefore, the development of an ESP requires consideration of the laws and regulations within the jurisdictions where data is transmitted, resides, or is processed. This includes laws governing privacy, security, cybercrime, economic espionage, protection of intellectual property and trade secrets, data retention, and data destruction. Beyond this, other types of security requirements flow from non-disclosure agreements, contracts with third parties, and the need to protect confidential and proprietary information.

Effective governance requires an understanding of the compliance and legal issues at hand. The EU Data Protection Directive (DP Directive), which governs the EU's 27 member states and the three countries in line for accession, has had the greatest impact on privacy laws, regulations, and corporate operations around the globe. The DP Directive governs the collection, use, retention, and transmission of personally identifiable information (PII). PII can only be collected if the person has agreed to the collection of the data (also known as "opt-in").

Under the DP Directive, the collection of the data is limited to that which is necessary. It can be used only for the stated purpose, the data can be kept only as long as necessary, and it must be kept up-to-date and be accessible to the person from whom it was collected. The data also must be fairly and lawfully processed, with a means for the individual to object to the processing.

The EU also restricts the transfer of PII to countries outside the EU unless at least one of the following conditions is met:

- The person has given clear and informed consent to the transfer of the data.
- The entity receiving the data is subject to approved EU contractual clauses regarding protection of the data.
- The entities receiving the data are part of a group of entities operating under Binding Corporate Rules (BCR) approved by the EU Member States.

- The data is being sent to an entity in a country which has received an “adequacy” ruling from the EU Commission that the laws of the country afford protections to the data that are equivalent to those in the DP Directive; *or*
- The data is being sent to an entity in the U.S. that is a registered member of the Safe Harbor Program, administered by the U.S. Department of Commerce and enforced by the Federal Trade Commission.

Several other countries have adopted similar legislation and impose comparable restrictions on the transfer of PII outside their borders.

Canada, one of the countries that has received an “adequacy” ruling from the EU, allows Canadian provincial laws that are deemed to be “substantially similar” to its Personal Information Protection and Electronics Document Act (PIPEDA), to trump PIPEDA. According to the Canadian Privacy Commissioner, provincial laws may be deemed to be “substantially similar” if they are “equal or superior to PIPEDA in the degree and quality of privacy protection” provided [Westby 04b].

The U.S. privacy framework does not have an omnibus privacy law like the EU and Canada. To the contrary, it is quite fractured, with both state and federal laws protecting various *types* of data, such as driver’s license and social security numbers, cable television and telephone records, school records, insurance documents, and mailing lists. Other laws protect industry-specific information, such as financial and medical/health data. In addition, the federal Electronic Communications Privacy Act (ECPA) protects electronic communications records of public communications providers (cable, phone, telephony, and internet service providers) and restricts access by governmental entities to those records [Westby 04b].

The Asia-Pacific Economic Cooperation forum (APEC) has developed a hybrid privacy framework that is between the U.S. and EU models. The APEC Privacy Framework (Framework), however, is voluntary. There are certain flexible aspects of the framework that may be implemented by the adopting country to best suit its culture and existing laws and regulations.

The Framework anticipates cross-border data flows, commercial use of information, and “follow-the-sun” global operations, with data flowing across borders on a continual basis. It is certain to impact global operations and cross-border data flows since the 21 APEC member countries include the U.S., Canada, Mexico, Chile, Peru, Russia, and Australia [APEC 05].

In addition to privacy considerations, laws pertaining to security breaches also impose complex compliance requirements. Over thirty U.S. states have enacted security breach notification laws, requiring entities to notify persons if their PII has been breached. The requirements under these laws vary, with some of them applying only to public sector entities, some requiring notification only if the data was not encrypted, and others using a risk-based approach that requires notification only if the risk to the individual warrants it. The EU is considering a security breach notification requirement that would require notification of breaches to regulatory authorities. As noted earlier in this chapter, some laws and regulations, such as the GLBA and HIPAA, require security measures be taken to protect certain types of data.

Intellectual property and confidential and proprietary data have special security considerations. Corporations must take care to ensure that internal steps are taken to protect valuable data and satisfy the legal thresholds of the U.S. Economic Espionage Act of 1996 (EEA) or various other state and federal laws. Export control laws require similar measures to ensure that employees do not transfer controlled information without the appropriate license [Westby 03].

Data *retention* laws that require an organization to keep certain data for set periods of time are imposing yet another level of consideration for governance and ESPs. In December 2005, the EU Data Retention Directive was adopted by the EU parliament, with Member State compliance required by September 15, 2007. In the U.S., Colorado has adopted a data retention law and 49 of the 50 state attorneys general are encouraging the adoption of a national standard for data retention to assist the investigation of online sexual predators [Smedinghoff 06].

At the federal level, communication providers can be required to *preserve* data relating to a particular investigation upon issuance of a court order to do so. All entities are required by the Federal Rules of Civil Procedure to preserve data relating to pending litigation or if an entity has reason to believe or know that litigation may occur. The preservation of data requires an organization to keep and not destroy certain data related to an investigation, legal matter, or specific action until the matter is resolved and destruction of the data is allowed.

In addition, banking regulators and the SEC have adopted regulations regarding the duty to securely destroy data. These laws and regulations usually require that entities take measures to guard against unauthorized access to or use of the data during or after its destruction. Other data destruction laws require destruction of some business records after a certain amount of time [Smedinghoff 06]. For example, federal agencies are required to destroy various types of records after being held for a set period of time. These types of data destruction requirements impact the development and sustainment of ESPs.

Cybercrime laws and response scenarios create numerous governance considerations. The interdependencies between privacy, security, and cybercrime cannot be understated. *Quite simply, privacy compliance requirements are dependent upon effective security, and security and privacy breaches are cybercrimes. Thus, effective oversight of an ESP requires the blending of requirements for privacy, security, and cybercrime* [Westby 05].

Cyber criminal activities often cross borders simply due to the nature of internet protocol technology. Therefore, investigations related to local transactions can involve cumbersome international legal filings and requests just to obtain cooperation with international law enforcement. Even though cyberspace has no borders, law enforcement, prosecutors, government officials and diplomats do.

The amount of cooperation received from other countries is often dependent upon whether the foreign country [Westby 03]

- has a multiple lateral assistance treaty (MLAT) with the requesting country (if not, the time-consuming letters rogatory process must be followed. It consists of requesting government-to-government assistance through the foreign country's courts.)
- requires the act to also be a crime in their jurisdiction (dual criminality)

- imposes conditions on extradition
- has a 24/7 point of contact to receive assistance requests
- has trained and skilled law enforcement capable of the search and seizure of electronic evidence
- has adequate rules of criminal procedure to address chain of custody and evidentiary considerations

The lead team is responsible for developing a Table of Authorities listing all applicable laws, regulations, directives, contracts, and other legal requirements applicable to the organization's assets and systems.

3.2.3.2 Map Assets to Table of Authorities

Once compliance requirements have been identified, it is important to map their applicability to the inventory of digital assets. Risk management measures, including categorization of assets, determination of controls, and the development of policies and procedures, will be undercut or ineffective if compliance requirements are not correctly linked to the assets. This map helps identify training requirements or needed technical tools. This is a task jointly undertaken by the GC, CSO, and CPO, with the GC having the primary lead.

3.2.3.3 Map and Analyze Data Flows

The CPO has lead responsibility for mapping data flows and is assisted by the CSO, BM, and AO as needed. The mapping of data flows across jurisdictions helps identify compliance and liability risks and is invaluable in categorization and control activities. The map guides the X-team in ensuring that appropriate policies and procedures are in place in the various jurisdictions. Data flow maps provide valuable input to BLEs in strategic planning and decision-making, as they can visually "see" the flow of their operational information. Data flow maps are helpful to BLEs in understanding the impact of certain operational shifts. They identify what data is transmitted to jurisdictions without privacy protections or cybercrime laws and show what alternative measures may be available, such as contract clauses, to help organizations meet their compliance obligations.

Legal publications and guides, often developed by law firms, are useful tools in analyzing cross-border data flows and legal risks and compliance obligations. [Baker 06, EPIC 06]

3.2.3.4 Map Cybercrime and Notification Laws and Cross-border Cooperation to Data Flows

Data flow maps serve as the starting point for mapping cybercrime and security breach notification laws that apply in the jurisdictions where the data is sent. This activity is led by the GC, with the assistance of the CSO, CPO, and BLE as needed. This mapping includes information specific to each jurisdiction, such as the laws that apply, cooperation considerations (such as whether a Mutual Legal Assistance Treaty (MLAT) is in force or the CoE Cybercrime Convention has been ratified), notification requirements, and more.

It helps organizations to

- work through potential response scenarios
- plan international cooperation with law enforcement
- understand the jurisdictional considerations in investigations and prosecutions
- establish points of contact and build relationships with necessary public and private sector entities
- ensure policies, procedures, and technologies help mitigate risks and ensure the organization meets the legal thresholds of cybercrime laws.

This mapping is a key input into the development of policies and procedures as well as incident response and crisis communication plans so it is useful in strategic planning and business unit management.

3.2.3.5 Conduct Privacy Impact Assessments and Privacy Audits

The CPO leads the development of privacy impact assessments (PIAs) for all PII that is being collected, processed, and stored. PIAs are useful in understanding the full impact of data flows and mitigating risks associated with PII. The U.S. Government's Office of Management and Budget defines a PIA as the following:

An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks [Bolton 03].

The U.S. Department of Homeland Security has published guidance on the development of PIAs that is equally applicable in the private sector environment [DHS 06].

Changes in operations and the legal landscape require constant and detailed attention to ensure that new risks are not left unchecked and that all relevant documentation is updated through effective change management procedures.

Few operations remain static over the course of a year. Moving operations to a different location or to an outsource provider, changing authentication technology, increasing remote access to PII, and other technological or operational changes can have a significant impact on privacy compliance.

CPOs should conduct periodic privacy audits to verify that privacy compliance requirements are being met, policies and procedures are being complied with, and that operational and technological changes have been properly handled and have not impacted privacy protections. The GC and CSO may assist in these activities as needed.

Artifacts: The artifacts produced during these activities include the following:

- Table of Authorities
- Mapping of Assets and Authorities

- Mapping and Analysis of Data Flows
- Mapping of Cybercrime and Notification Laws and Cross-Border Cooperation
- Privacy Impact Assessments
- Privacy Audit Report

3.2.4 Governance Category Activities #4 – Assessments and Strategy

- Conduct Threat, Vulnerability, and Risk Assessments (including System C&As)
- Determine Operational Criteria
- Develop and Update Security Inputs to the Risk Management Plan
- Develop and Update Enterprise Security Strategy (ESS)

3.2.4.1 Conduct Threat, Vulnerability, and Risk Assessments

After compiling information describing digital assets and legal and compliance requirements, the next step in the development and sustainment of an ESP involves conducting threat, vulnerability, and risk assessments. The CSO leads the assessment activities, with assistance from the BLEs, BM, and OP, with oversight by the BRC. If a certification of the system is being performed, the CA will share a lead role with the CSO.

In their insightful publication, *Information Security Governance: What Directors Need to Know* [IIA 01], the Institute of Internal Auditors noted:

Like due diligence, there is no end to assessing information security. Technology’s rapid pace necessitates continuous upgrading and maintenance. Management, with appropriate board oversight, must determine the economic “point of no return” in assigning resources. There is a continuous cost/benefit trade-off and a need to prioritize and focus resources on assets that must be protected.

Governance of digital assets is about managing the risks that compromise those assets to the detriment of the organization. FISMA requires federal agencies and departments to manage information security commensurate with the “risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction” of information and systems [FISMA 02]. This involves balancing the operational and economic costs of security controls with gains in competitiveness and other organizational benefits derived from protecting the digital assets that support the business mission and functions.

NIST [Stoneburner 02] defines risk as “a function of the *likelihood* of a given threat-source’s exercising a particular vulnerability, and the resulting impact of that adverse event on the organization.”

That is, risk exists where a threat intersects with a vulnerability [Bowen 06]. NIST’s *Risk Management Guide for Information Technology Systems* (NIST 800-30) [Stoneburner 02] neatly explains this definition for risks to IT systems:

To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT

system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of a vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the IT system components and data).

It is impossible to conduct an effective organizational assessment based on risk and magnitude of harm without collectively analyzing the risks associated with each system. Effective risk management must, therefore, be integrated into the system development life cycle (SDLC) [Grance 04b].

There are five phases in an SDLC: initiation, development or acquisition, implementation, operation or maintenance, and disposal. A system can be within several phases at one time, which is not problematic because the same iterative risk assessment process is applied at each phase [Stoneburner 02]. It may be tempting for management to incorrectly determine that governance does not extend this far into the ESP process and turn this risk assessment activity over to technical experts. NIST [Bowen 06] notes:

[T]he risk management process should not be treated primarily as a technical function carried out by the information security experts who operate and manage the information security system, but as an essential management function of the organization that is tightly woven into the system development life cycle....

Risk assessments can be performed in various ways to meet the needs of the organization. The depth of a risk assessment varies according to the criticality and sensitivity of the system, which is based upon categorization of the applications it runs, the networks it uses, and the information it stores and transmits (for more information, refer to section 3.25, *Governance Activities during Integration and Operations #1 – Categorization and Controls*, later in this chapter). *It is through this process that organizations identify their “critical digital assets,” i.e., those assets that are critical to the organization’s viability, profitability, and sustainability.* Examples of critical assets can include trade secrets, important processing applications, proprietary distribution and supply lists, customer files, just-in-time inventory systems, early warning systems, accounts receivable data, and the like.

System risks may be managed through system self-assessments and the disciplined and structured certification and accreditation (C&A) process [Swanson 01, NIST 05, Ross 04]. System C&As support the risk management process and are performed on a regular basis. NIST guidance calls for C&As to be performed on government systems every three years. The term security certification refers to the assessment of the agreed-upon security controls in an information system to determine the effectiveness of those controls. The certification documentation indicates the effectiveness of controls including policies and procedures, and identifies weaknesses, vulnerabilities, or deficiencies that need to be addressed. The documented results of the certification process identify the risk and magnitude of harm the system poses to the enterprise missions. The BLE uses the risk self-assessment and C&A results to decide whether to issue an accreditation letter authorizing the system to operate, granting interim authority to operate, or denying authority to operate. While C&As as defined by NIST are for U.S. government systems, this structured approach can be applied to any system.

As examples, Figure 3.1 in NIST 800-30 [Stoneburner 02] and CERT's OCTAVE²⁵ (Operationally Critical Threat, Asset, and Vulnerability Evaluation) describe useful risk assessment processes and methods that are instructive and applicable to all organizations.

3.2.4.2 Determine Operational Criteria

The BLE has the lead in determining operational criteria, with assistance from BMs. Operational criteria are determined in part by the risk assessment process and in part by the BLEs and the operational and strategic goals of the enterprise. Criteria can include system availability and bandwidth requirements, restrictions on access to assets, system interconnectivity requirements (internal and external), remote or third party access, physical parameters (such as exceptionally hot or dirty environments or public access to operational areas), etc. The need for security technical solutions, such as encryption software, identity management systems, and monitoring and anomaly detection systems are often determined by operational criteria.

The BRC has the responsibility to ensure that (1) operational criteria align with risk assessments and the organization's risk management plan, and (2) the ESP supports the operational criteria.

3.2.4.3 Develop and Update Security Inputs to the Risk Management Plan

The risk management plan (RMP) is an organization's overall governing risk plan. The RMP encompasses the full range of risks to people, products, plants, processes, policies, procedures, systems, networks, and information (P6STNI) [Westby 05, see also ISACA 05a]. Risk assessments are the underpinnings of the RMP; they are analyzed and form the basis for the avoidance, acceptance, or mitigation of identified risks. RMPs may accommodate or mitigate certain risks through controls or insurance. Security inputs to the RMP are developed by the CSO, with the assistance of the CPO, CIO, and GC and oversight by the BRC.

3.2.4.4 Develop and Update Enterprise Security Strategy

An enterprise security strategy (ESS) supports the organization's RMP and performance goals. It is developed by the CSO, with input from the CPO and oversight by the BRC. The ESS serves as a long-range (usually three- to five-year) plan which guides the organization in the deployment and sustainment of its ESP. The ESP requires continual review and improvement to accommodate (a) changes in laws, regulations, directives, or contractual obligations; (b) shifts in business unit mission or corporate strategy and operations; and (c) new security risks, technological innovations, or changes in system architecture requirements. Absent dramatic operational shifts, the ESS remains relative static and, while referenced frequently and reviewed annually, it is revised at set intervals.

Artifacts: The artifacts produced during these activities include the following:

- Risk Assessments
- Certification Letters
- Operational Criteria

²⁵ <http://www.cert.org/octave/>.

- Security Inputs to Risk Management Plan
- Enterprise Security Strategy

3.2.5 Governance Activities during Integration and Operations #1 – Categorization and Controls

- Categorize Assets by Levels of Risk and Magnitude of Harm
- Determine and Update Necessary Controls
- Develop and Update Key Performance Indicators and Metrics

3.2.5.1 Categorize Assets by Levels of Risk and Magnitude of Harm

The categorization of assets is one of the most important steps in the development and sustainment of an ESP. It is carried out by the CSO and BLE, with assistance from the CPO, GC, and BM as needed and with oversight by the BRC. The importance of the BLE in this process cannot be overstated. Business missions and critical assets are protected through proper categorization. Only the BLE understands the importance of these assets and assumes the risk they pose to the organization. The CSO plays a guiding role and ensures that a consistent approach is used in the categorization process across all business units and that the process is completed in a timely manner.

This activity is of such a critical nature that FISMA mandates that federal agencies follow the standard developed by NIST for security categorization, the *Federal Information Processing Standards Publication 199 (FIPS 199)*.

The FIPS 199 standard [FIPS 04] notes:

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 obligations, maintain its day-to-day functions, and protect individuals.

Using the threat and vulnerability inputs derived from previous activities, categories are determined based upon the impact that the compromise of an asset would cause to the organization. Categories are assigned to all assets in a system based upon three *risk factors*: confidentiality, availability, and integrity (CAI). *Categories* of High, Moderate, Low, or Top Secret, Secret, and Confidential are the usual designations for tiers of protection. NIST uses the former, which this chapter uses as well.

Databases, applications, and networks are each categorized based on impacts and losses that can result from compromises of confidentiality, availability, and integrity [Westby 05, FIPS 04]:

- Confidentiality: maintaining restrictions on access and disclosure, including protections for PII
- Integrity: protecting against data sabotage, destruction, or modification and preserving qualities of non-repudiation and integrity of data
- Availability: providing reliable access to the asset

General rules of thumb in making category determinations are the following [Barker 04a, Barker 04b, Westby 04b]:

- Low: the loss of confidentiality, integrity, or availability is expected to have a limited impact on operations, assets, or personnel. The incident would degrade operations to the extent that primary functions could still be performed but they would be less effective. There would be minor harm to assets or individuals and minor financial losses.
- Moderate: the loss of confidentiality, integrity, or availability is expected to have a serious impact on operations, assets, or individuals. The incident would significantly degrade operations to the extent that primary functions could still be performed but the effectiveness would be substantially reduced. There could be significant damage to assets, and substantial financial losses, and personnel could be seriously harmed (but no life threatening injuries or death)
- High: the loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic impact on operations, assets, and personnel. The incident would impact operations such that primary functions may not be able to be performed, assets could suffer major damage, major financial losses could be incurred, and personnel could lose their life or suffer life threatening injuries.

Table 3 indicates a sample categorization of a medical claim system that is connected to several health provider systems. The highest category (high, moderate, low) based on the three factors (CAI) establishes the security category for the asset. Using the two database assets in the table as an example, the claims database is assigned a confidentiality category of low because there is no PII or other protected information on this database. The integrity of the claims is more important, however, so that category is deemed to be moderate.

Disruptions to the availability of the claims database would only moderately impact the organization, so a moderate category is assigned. Since the highest category assigned is moderate, that is also the final category for that asset. The patient database, however, does contain both identifying information and sensitive PII (race, age, medical diagnosis, and treatment). Therefore, its categorization levels are high for confidentiality and integrity, but moderate for availability since disruptions would only moderately impact the organization. Its final categorization is high.

Table 3: Categorization of a Medical Claim System

	Asset	Confidentiality	Integrity	Availability	Category
Networks	General Support Network	Low	Low	Moderate	Moderate
Applications	Claims Processing Application	Low	Moderate	Moderate	Moderate
Databases	Claims Database (no PII)	Low	Moderate	Moderate	Moderate
	Patient Database	High	High	Moderate	High

3.2.5.2 Determine and Update Necessary Controls

Controls could be considered the gates, guards, and locks protecting IT assets. They are determined by the CSO, with assistance from the CPO, BLE, BM, and GC as needed, and oversight by the BRC. Since BLEs assume the risk for their systems, it is important that BLEs and BMs take more than a passive role in this activity to ensure controls are effective, are consistent with how business operations are performed, and are understood by employees. Security controls are defined as the following [Ross 05a]:

The management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

There are three classes of controls: technical, managerial, and operational. Technical controls can be incorporated into the hardware, software, or firmware. Non-technical controls support management and operational activities or processes. Controls can be used for various purposes: to support an activity or function, to prevent an event from occurring, to detect an event, or support recovery efforts [Westby 05]. Baseline controls are used to achieve the minimum security needed for a system [Ross 05a].

Security controls have three components [Ross 05a]:

- Control section – a concise statement regarding the specific security action or practice required to protect some aspect of an asset. Organizations are allowed flexibility in determining the protections needed.
- Supplemental guidance – additional information regarding the security control, for example, frequency of backups or the transfer rate required to restore a system.
- Control enhancements – statements describing additional capabilities or functionalities needed from a control.

One of the leading de-facto standards for the definition and audit of IT controls (including security) is CobIT²⁶ (Control Objectives for Information and related Technologies) [ITGI 05b]. CobIT describes a framework for IT governance and IT audit. It is intended to ensure the effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of information and the systems used to process information. CobIT is organized into four domains (planning and organization, acquisition and implementation, delivery and support, and monitoring), 34 high-level control objectives, and 318 detailed control objectives. [Allen 06d] Other leading standards that define IT and security controls include ISO 17799 [ISO 05a], NIST's Recommended Security Controls for Federal Information Systems [Ross 05a] and its accompanying Annexes, and the Federal Information System Controls Audit Manual (FISCAM) [GAO 99].

3.2.5.3 Determine and Update Key Performance Indicators and Metrics

CSOs must strive to establish security key performance indicators (KPIs) and monitor and measure the effectiveness of security controls. The CSO has lead responsibility for this activity, with assistance from the BLE, BM, OP, and CIO as needed, with oversight by the BRC. KPIs are preset performance points, or measures, used to determine whether the desired level of security is being achieved. Performance metrics can be assigned at the organizational and system level.

Organizational KPIs help measure an organization's fulfillment of its strategic goals and objectives [Chew 06].

Security KPIs at the operational level can include the number of security incidents, the number of times a policy was violated, the number of attempted intrusions to a system, the cost of system down time, and more. Operational metrics from security technologies such as anti-virus software, intrusion detection/intrusion prevention systems, enterprise security management consoles, log analysis, and the Center for Internet Security²⁷ testing tools are valuable aids in evaluating technical controls. (See also a reference in the bibliography for these chapters from the Corporate Information Security Working Group [CISWG 04] for a set of security metrics at the governance, management, and technical levels.)

Security metrics are based on security goals and objectives and are quantifiable measurement data regarding the effectiveness of security controls. The BRC and senior management must ensure that the metrics accurately reflect the effectiveness of the ESP and support the organization's strategic and operational processes [Westby 05, Swanson 03].

NIST has developed excellent guidance on the assessment of security controls that may be helpful to private organizations in undertaking this activity [Ross 05b].

²⁶ <http://en.wikipedia.org/wiki/COBIT>

²⁷ <http://www.cisecurity.org/>

Artifacts: The artifacts produced during these activities include the following:

- Categorization of Assets
- Assignment of Controls
- Key Performance Indicators and Metrics

3.2.6 Governance Activities during Integration and Operations #2 – Crisis and Incident Planning

- Develop, Update, and Test Incident Response Plan
- Develop, Update, and Test Crisis Communication Plan
- Develop, Update, and Test Business Continuity and Disaster Recovery Plan
- Develop, Update, and Verify Third Party and Vendor Requirements

3.2.6.1 Develop, Update, and Test Incident Response Plan

The incident response plan is one of the most important artifacts in an ESP. It is the responsibility of the CSO, with oversight by the BRC. The CIO, BLE, GC, and PR assist in the development of the IR plan. The BLE must ensure that the incident response plan supports business goals and objectives and is in line with the risk that the BLE has accepted for the system. In addition, the BLE needs to guard against IR activities that may be overly disruptive to business operations.

The IR plan can be viewed as the first line of defense in an ESP. Incident response plans must accommodate all kinds of threats to assets committed by both insiders and those external to the organization: viruses, worms, and other malicious code; denial of service attacks; economic espionage and theft; unauthorized access; inappropriate usage; sabotage; destruction of data and more. Some incidents can develop into crises while others can undermine the effectiveness of an ESP if not properly managed. Therefore, prioritizing incidents is an important part of any IR plan.

An IR plan requires qualified personnel with assigned responsibilities consistent with SOD, policies and procedures, a communications plan, guidelines for preservation of evidence and forensic data, periodic reporting, and training.

Documentation of events and interactions with others is very important in managing incidents, analyzing responses, and improving response capabilities [Grance 04a]. (See also the CERT Computer Security Incident Response Team (CSIRT) home page²⁸ for additional guidance.)

Incident response plans play an important role in managing legal risks and liabilities. Lawsuits regarding cyber incidents are becoming more frequent, and how organizations respond to incidents can often significantly impact legal matters down the road. Increasingly, in-house and outside counsel are leading investigations of cyber incidents to ensure that appropriate forensic data is preserved and evidentiary considerations are taken into consideration. Additionally, counsel's lead role may, in certain circumstances, enable organizations to protect sensitive information under the claim of attorney work product or attorney-client privilege.

²⁸ <http://www.cert.org/csirts>

3.2.6.2 Develop, Update, and Test Crisis Communications Plan

PR takes the lead in developing a crisis communications (CC) plan, with oversight by the BRC. The CSO, CIO, and BLE assist as needed. Crisis communication plans go hand-in-hand with incident response and business continuity planning. It is essential that leaders work through communications in response to possible scenarios before they occur.

They should determine the following:

- Who will speak to employees, what information will be relayed, and over what medium (internet, internal or external website, telephone, etc.)?
- Who will interact with first responders (if required)?
- Who will speak to the press and who decides what will be said?
- Who will speak to investors and analysts?
- Who will speak to law enforcement and determine what information will be shared?
- Who will speak to regulators or other government officials?
- Who will manage cross-border communications?
- What is the central contact point?
- If a security breach occurs at a third party or outsource vendor, when will the client be notified and what will be the plan of communications?

While most incidents do not require all of the foregoing, it is the one incident that does that can result in damage to corporate reputation, market share, and stock price.

Clear lines of responsibility and SOD must be given careful consideration in the development of crisis communication plans, but there is no substitute for testing, evaluating, reviewing, and continually updating and maintaining IR and CC plans.

3.2.6.3 Develop and Update Business Continuity Plans and Disaster Recovery Plans

Risk management of IT assets necessarily involves ensuring that an organization has the ability to maintain or recover operations in times of disruptive or catastrophic events. The current buzzwords are “resilience” and “redundancy” – an organization’s ability to adaptively respond to disruptive events and tolerate being affected by them. The CSO, CIO, and BLE share responsibility for the development of BC/DR plans, with assistance from the BM and OP as needed and with oversight by the BRC. The BLE is integrally involved in the development, maintenance, and testing of BC/DR plans and is the interface point between IT and business operations to ensure operations are, in fact, continued in a manner consistent with the RMP and ESS. BC/DR plans serve as the foundation for policies, procedures, and processes that will guide an organization through an array of incidents and keep it viable, profitable, and competitive.

Fortunately, BRCs and CSOs can now look to excellent guidance in these efforts from best practices developed by NIST, ISO, British Standards Institution (BSI), and other organizations. BSI, the original developer of the standard for information security, has developed a standard for business continuity, BS 25999 [BSI 06].

Regarding management's role in BC, BS 25999 notes:

Top management, especially in a large multinational organization, might not be directly involved; however, top management accountability through the chain of command is manifest. In a small organization, top management might be the owner or sole proprietor.

BS 25999 does not, however, cover civil emergencies and related emergency planning. Because of the possibility of events such as natural disasters and terrorist attacks, organizations must prepare for all types of emergencies. While a plan does not need to be developed for every possible outage, it is essential that plans be developed for high-impact scenarios.

The designation of recovery time objectives (RTO) is an important control [BSI 06]. In addition, technology recovery plans for restoring IT services to an organization – often through an alternate location – must dovetail with business continuity plans [Westby 05]. It is important to analyze the scalability of incidents and manage the risks to prevent incidents from becoming crises. BC planning must take into account outsourced activities since they may carry a higher risk than those performed internally [BSI 06].

The artifacts developed in the ESP are important to BC/DR planning. The inventory of assets, particularly those assets that have been identified as critical to the organization's goals, objectives, strategies, and competitiveness are key inputs to the development of BC/DR plans [BSI 06, Westby 05]. In addition, the system descriptions are valuable, and asset owners can help determine how systems are to be handled in a BC/DR scenario.

Once a BC/DR plan has been developed, it is essential that it be tested through effective exercises, evaluated, and kept up-to-date. Exercises should involve critical stakeholders and test the technical, logistical, administrative, procedural and operational systems of the BC/DR plan [BSI 06].

3.2.6.4 Develop, Update and Verify Third Party and Vendor Requirements

This CSO and CIO share the lead responsibility for this activity, with input from the BLE and oversight by the BRC. It is important that organizations step back and analyze what operations are being performed by third parties, such as business partners, suppliers, and vendors. The priorities and responses that might take place internally may not be appropriate or the same outside an organization. The work may carry higher risk because it is performed by an outside party, requiring added controls, reviews, policies and procedures, or governance measures.

For example, leaders may not ever know about a security breach of corporate data at a vendor location unless specific requirements are in place governing such circumstances. Likewise, a vendor may make statements to the press, share information with law enforcement, or destroy or fail to preserve logs and important evidence. In addition, grave and important security considerations surround the development of software and hardware and the risk of built-in backdoors or exploits (hidden code that permits unauthorized access). Thus, it is important that ESP requirements be transferred to third parties and vendors and modified where appropriate to manage risk. Controls, metrics, reporting, auditing, and effective governance structures help organizations analyze and verify whether their security program is effectively implemented by outside parties and risks are managed or mitigated.

Artifacts: The artifacts produced during these activities include the following:

- Incident Response Plan
- Incident Response Plan Test Report
- IR Reports
- Crisis Communications Plan
- Crisis Communications Plan Test Report
- CC Reports
- Business Continuity/Disaster Recovery Plan
- BC/DR Plan Test Report
- Third Party and Vendor Requirements for IR, CC, and BC/DR
- Third Party and Vendor Requirements Verification Report

3.2.7 Governance Activities during Integration and Operations #3 – Security Plan

- Develop and Update Enterprise Security Plan
- BRC Approval of Enterprise Security Plan

3.2.7.1 Develop and Update Enterprise Security Plan

The foregoing activities have each contributed to the development of a security plan that serves as the overarching plan for the organization. The development of the plan is the primary responsibility of the CSO, working with the X-team, and designated operational personnel, with oversight by the BRC. The plan is developed based on the business unit security plans (if the organization is large enough) and requirements from system security plans. This “bottom-up” approach (from system plans upward), combined with the more “top-down” input from the RMP, ESS, and top-level policies, converge in the process of developing the enterprise security plan. This methodology helps ensure that security requirements support business goals and objectives, rather than constrain them. It is important that the same critical inputs discussed in Chapter 2, “Defining and Effective Enterprise Security Program,” Figure 2, are factored into the enterprise security plan so that managerial, legal, operational, and technical considerations for the entire organization are accommodated.

3.2.7.2 Approval of Security Plan

The BRC has the responsibility for final approval of the enterprise security plan. This involves a close review of the plan, including verifying that it is in line with the RMP, ESS, and top-level management policies.

In addition, the BRC should undertake an assessment regarding whether [Westby 05]:

- all system security plans have been integrated into the plan
- critical assets are adequately protected
- baseline security requirements are met

- controls, metrics, and governance processes are adequate
- appropriate SOD (or counterbalancing approvals or checkpoints) is in place for more detailed security responsibilities
- the BC/DR, IR, and CC plans are incorporated into the plan

The BRC signs off on the enterprise security plan through a formal letter of approval of the plan. This letter is an important artifact in the ESP.

Artifacts: The artifacts produced during these activities include the following:

- Enterprise Security Plan
- BRC Approval Letter for the Enterprise Security Plan

3.2.8 Governance Activities during Implementation and Evaluation – Implement and Train

3.2.8.1 Develop and Update ESP Implementation and Training Plans

The truth to the expression “security is only as good as its weakest link” is often realized when excellent security programs fail due to the lack of proper implementation and training of personnel. In 2002, the FTC initiated action against Eli Lilly for its inadvertent failure to uphold a privacy promise it had made to patients using Prozac, even though it had a policy covering the operational processes. The FTC’s complaint alleged the company’s claim of privacy and confidentiality of this information was deceptive because of “failure to maintain or implement internal measures appropriate under the circumstances” to support the policy” [FTC 02a]. According to the FTC, Eli Lilly failed to [FTC 02a]:

- provide appropriate training for employees regarding consumer privacy and information security
- provide appropriate oversight and assistance for the employee who mistakenly disclosed the identities of the patients through a “string listing” of patient email addresses
- implement appropriate checks and controls on the process

The consent decree required Lilly to establish a four-part security program with reasonable and appropriate administrative, technical, and physical safeguards to protect PII against any reasonably anticipated risks to its security [FTC 02b]. The FTC’s strong message in the Lilly case was that policies on paper are not enough; people need to be trained and the policy needs to be integrated into daily operations through effective procedures, with appropriate controls put in place to help prevent mistakes.

The CSO has the primary responsibility to develop the implementation plan with oversight by the BRC. X-Team involvement from the CPO, HR, BLE, PR, CIO, and GC is critical. The BLE plays a key role in ensuring that business unit personnel are engaged and understand the importance of policies and procedures and the associated training they will receive. Additional input is provided by the BM, AO, and OP.

The training plan must go beyond security awareness and identify target audiences that require specialized training regarding privacy and security responsibilities. For example, boards and senior management must receive training regarding their governance responsibilities in developing and sustaining ESPs.

Business managers require another level of security training, and so on, down to the training of operational personnel who handle, transmit, and have custody of data. Therefore, a variety of training modules must be developed and delivered to a wide range of personnel according a planned schedule. Many personnel will need to receive more than one type of training (e.g., security awareness, security governance, security of operational data during specific processes, and the like).

Artifacts: The artifacts produced during this activity include:

- Implementation Plan and Results
- Training Plan and Schedule

3.2.9 Governance Activities during Capital Planning and Reviews/Audits #1 – Funding

3.2.9.1 Determine Security Business Case, Return on Investment, and Funding

One of the most perplexing areas of cyber security is

- understanding how to make a business case that justifies investment and expenditures on security
- calculating return on investment
- determining the appropriate allocation of resources for the development, implementation, and sustainment of the ESP

The U.S. Office of Management and Budget has issued memoranda and NIST has published guidance regarding integrating security requirements into the SDLC and capital planning and investment processes for all federal systems. This area is decidedly unsettled, however, outside the U.S. government. NIST Special Publication 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process* [Hash 05], offers invaluable guidance that, for the most part, can be adapted to the private sector environment and budgetary process.

Research conducted by Lawrence Gordon and Martin Loeb at the University of Maryland [Gordon 06] advances the discussion regarding the economics of cyber security and its return to organizations.

All too often, the allocation of financial resources for ESPs is based upon

- limited input from a couple of executives or reports
- what has been spent in previous years
- whether any serious breach has occurred before

- whether security measures are a compliance requirement that has criminal or serious consequences
- what funds other business units are willing to throw into the “security pot”

Each of these is an invalid approach, and collectively, they leave an organization vulnerable to a full range of risks to its operations, processes, people, facilities, networks, applications, and data. Instead, financial resources must be allocated to support the following:

- ESP activities (including security requirements)
- POAM corrective actions
- training programs
- monitoring and enforcement activities
- special assistance, such as forensic expertise, outside legal counsel, technical experts
- periodic (no less than annual) reviews of the ESP and ongoing maintenance activities

The CSO and CFO share the lead responsibility for this activity, with oversight by the BRC. The resources allocated to the ESP are recommended by the BRC and approved by the board of directors.

Artifacts: The artifacts produced during this activity include the following:

- ESP Security Investment Requirements and ROI Analysis
- Board Approved Budget for the ESP

3.2.10 Governance Activities as part of Capital Planning and Reviews/Audits #2 – Reviews and Audits

3.2.10.1 Conduct Formal Review and Audit of ESP

Formal reviews of an ESP, business unit security plans, and system security plans are essential, lest an organization lose control of its digital assets and processes and be subject to increased risk. Changes in business operations, top-level policies, compliance requirements, technological vulnerabilities and innovations, shifts in personnel, and budgetary limitations can impact every aspect of business operations, including the security program. The artifacts produced in the development of an ESP serve as important risk documentation and guide courses of action throughout the year. It is essential that they be kept up-to-date and be viewed as trusted resources. These artifacts must evolve with business operations, accommodate new legal liabilities and risks, and stay aligned with the RMP and ESS.

Formal reviews of the ESP should take place no less than once per year. The CSO leads the review, with assistance from the X-team and oversight by the BRC. The BRC approves the formal review report. Simultaneously, the board audit committee (BAC) and internal and external auditing personnel may be conducting annual audits of the ESP. The results of the reviews and audits serve as valuable cross-checks and help limit risks and liabilities. They help identify deficiencies and ensure policies and procedures are complied with and controls are effective.

The BAC and internal and external auditors conduct an independent review of the ESP and issue their own reports. In the course of their audit work, they validate and verify that

- the proper governance structure is in place
- the RMP, ESS, and enterprise security plan are followed
- risk assessments are adequate and linked to the RMP, ESS, and enterprise security plan
- roles and responsibilities are fulfilled and SOD is effective
- compliance and legal requirements are identified and met
- privacy impact assessments are complete and privacy requirements are met
- the inventory of assets is complete, up-to-date and properly categorized
- controls and KPIs are effective and properly implemented
- best practices and standards are followed and security configuration settings are defined and deployed
- policies and procedures are current and compliance is monitored and enforced
- supporting plans (BC/DR, IR, CC, and change management) are tested and followed
- third parties and vendors are meeting their requirements
- systems within the program are certified and accredited
- material system weaknesses are identified and addressed through POAMs
- security investments are adequate and subject to ROI or equivalent analysis, as for other business investment decisions, and security ROI is tracking to plan
- the findings of previous audits and reviews have been incorporated into the current RMP and enterprise security plan and deficiencies and material weaknesses have been corrected

Artifacts: The artifacts produced during these activities include the following:

- Report on Annual Review of ESP
- Report on Annual Audit of ESP (internal report and external auditor reports)

3.3 ADDITIONAL CONSIDERATIONS

3.3.1 Keeping Up With the Pace of Technology

Security of assets evolves with technological innovations. Just as ESPs become stable, new technologies – as well as new vulnerabilities and threats – require BRCs and X-team members to adapt to the pace of technology change and ensure that the ESP stays ahead of the risks that come with new innovations. Today, the digital revolution is impacting organizations in a much more subtle way than the internet did in the mid-1990s.

The following areas require special attention because they pose particular security risks to enterprises and may require changes to the way the organization approaches the management and security of its assets:

- mitigating the exploitation of new technologies
- security of web services
- securing radio frequency identification (RFID) systems
- personal identity verification (PIV) and identity management
- personal digital assistant (PDA) and other mobile devices (security of the device, safeguarding information on the device, and forensics regarding intrusions or attacks)
- security of Voice Over Internet Protocol (VOIP) systems
- Security of wireless devices (802.11, Bluetooth, handheld devices)
- sanitization of media

NIST has published guidance in each of these areas that is useful to public and private sector organizations. In addition, it is important to understand the risks associated with new technologies either on the horizon or in early stages of deployment, such as virtualization of machines and grid computing.

Sources for keeping up to date on current and emerging attack trends include US-CERT's²⁹ Security Alerts and Current Activity and the SANS³⁰ Institute's list of Top-20 Internet Security Attack Targets.

3.3.2 Best Practices and Standards

As boards and corporate leaders approach the governance and development of ESPs, it is important that they carefully select and implement best practices and standards that are appropriate for the security of their business operations. Although not a comprehensive listing, some of the better known standards and guidelines for sound practices are listed below.

The good news is that these practices are, for the most part, consistent. Some organizations have undertaken valuable practice mappings that can be useful when acquiring and integrating systems that are documented based upon different standards [ITGI 05a].

- ISO/IEC 13335: Information Technology – Security Techniques – Management of information and communications technology security – 4 parts (1998-2004)
- ISO/TR 13569: Financial Services – Information Security Guidelines (2005)
- ISO/IEC TR 14516: Information Technology – Security Techniques – Guidelines for the use and management of Trusted Third Party services (2002)
- ISO/IEC 15408: Information Technology – Security Techniques --- Evaluation Criteria for IT Security (Common Criteria) – 3 parts (2005)
- ISO/IEC 15446: Information Technology – Security Techniques – Guide for the Production of Protection Profiles and Security Targets (2004)

²⁹ <http://www.us-cert.gov/>

³⁰ <http://www.sans.org/top20/>

- ISO/TR 15801: Electronic imaging – Imaging Stored Electronically – Recommendations for trustworthiness and reliability (2004)
- ISO/IEC 17799: Information Technology – Security Techniques – Code of practice for information security management (2005) [ISO 05a]
- ISO/IEC TR 18045: Information Technology – Security Techniques – Methodology for IT Security Evaluation (2005)
- ISO/IEC 20000: Information Technology – Service Management – 2 parts (2005)
- ISO/IEC 27001: Information Technology – Security Techniques – Information Security Management Systems – Requirements (2005) [ISO 05b]
- ISO/IEC 21827: Systems Security Engineering – Capability Maturity Model® (SSE-CMM®) (2002)
- BS 25999: Code of Practice for Business Continuity Management (2006) [BSI 06]
- COBIT 4.0 Control Objectives for Information and related Technology (2005) [ITGI 05b]
- IT Infrastructure Library (ITIL)³¹
- The Information Security Forum’s The Standard of Good Practice for Information Security³²
- NIST Special Publications³³
- The Payment Card Industry Security Standard³⁴
- U.S. Department of Defense Security Directives and Instructions³⁵

3.4 CONCLUSION

This chapter serves as a companion to Chapter 2, “Defining an Enterprise Security Program.” It provides a fairly detailed description of the activities that require governance action by senior leaders to develop and sustain an enterprise security program. The roles responsible for overseeing and conducting these activities range from members of the board of directors, the board risk committee, and the board audit committee to members of the organization’s cross functional X-team, including the general counsel, the chief risk officer/chief security officer, and business line executives.

Activities are defined in four categories: governance; integration and operations; implementation and evaluation; and capital planning and review. Governance-category activities establish the ESP’s organizational structure, roles and responsibilities and policy; identify assets and their ownership; determine security compliance requirements; and call for the conduct of risk-based assessments that result in a comprehensive enterprise security strategy.

³¹ <http://en.wikipedia.org/wiki/ITIL>

³² http://www.isfsecuritystandard.com/index_ns.htm

³³ <http://csrc.nist.gov/publications/nistpubs/index.html>

³⁴ <https://www.pcisecuritystandards.org/tech/index.htm>

³⁵ <http://www.fas.org/irp/doddir/dod/index.html>

Governance-based activities during integration and operations include asset categorization, determination of controls, and the identification of performance measures; the development of plans for incident response and business continuity; establishing security requirements for third parties; and developing the guiding plan for the enterprise security program.

Governance-based activities conducted during implementation include ESP rollout planning and training plan development. During capital planning and review, leaders are responsible for establishing a security business case, providing ESP funding, and conducting formal reviews and audits of the ESP.

This chapter briefly describes the artifacts the result from each activity. Selected artifacts are described in more detail in Appendices A, B, and C as follows:

- Appendix A: Board Risk Committee: Mission, Goals, Objectives, and Composition
- Appendix B: Cross-Organizational Team (X-Team): Mission, Goals, Objectives, and Composition
- Appendix C: Roles and Responsibilities for an Enterprise Security Program

These artifacts are presented as templates or examples that leaders can tailor for their organizations. They are not meant to stand alone—rather they should be interpreted in the context of these chapters.

3.5 SUMMARY

Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. To achieve a sustainable capability, organizations must make the protection and security of digital assets the responsibility of leaders at a governance level, not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance.

This implementation guide is designed to help business leaders implement an effective program to govern the security of their digital assets. Our objective is to help leaders make well-informed decisions about the important governance activities, roles and responsibilities, and outcomes discussed here.

Information and IT security risks increasingly contribute to operational and reputational risk. Leaders must understand the legal, technical, managerial, and operational considerations that converge in an enterprise security program. As with audit and compliance responsibilities, boards and senior officers need to thoroughly understand what it means to have effective security governance and how to bring it about. Tackling enterprise security governance is complex, and requires learning information and gaining knowledge that is missing in many organizations today.

The chapters and supporting artifacts presented in this guide provide a comprehensive roadmap of governance actions required to create and sustain an enterprise security program. They build upon and extend earlier work [Allen 05, Westby 05, Westby 04] and assume that leaders are in the process of implementing a governance- and enterprise-based approach to security for their organizations.

Appendix A: Board Risk Committee: Mission, Goals, Objectives, and Composition

Scope

This sample artifact describes the board risk committee mission, goals, objectives, and composition³⁶ as identified in Chapter 2, “Defining an Effective Enterprise Security Program,” Table 2 and Chapter 3, “Enterprise Security Governance Activities.”

Board Risk Committee (BRC) Mission

The mission of the board risk committee (BRC) is to protect

- the investment of the organization’s shareholders
- the organization’s assets (both physical and digital), people, operational processes, products, and reputation from internal and external risks

The BRC determines the organization’s tolerance or threshold for risk acceptance, avoidance, and mitigation. They also ensure that all risk plans align with corporate policies and strategic plans.

BRC Goals

In carrying out its mission, the BRC shall achieve the following goals:

- Establish a culture of risk management and security that permeates throughout the organization.
- Exercise oversight of enterprise risk management and security activities.
- Manage identified security risks according to asset criticality, likelihood of occurrence, and magnitude of harm and impact.
- Ensure an enterprise security program (ESP) is established and sustained with appropriate and adequate resources.
- Protect personnel, operations, information, and investments by emphasizing organizational resiliency.

³⁶ The mission and composition pertain to all BRC responsibilities. The goals and objectives of this sample artifact, however, apply only to the security of information, applications, and networks, and their grouping into systems. Supplemental goals and objectives would ordinarily be added for physical and personnel security.

BRC Objectives

The BRC shall accomplish the following objectives in meeting these goals:

- Establish an ESP governance structure for the organization, allocate responsibilities, and ensure segregation of duties according to industry best practices.
- Set the organization's cultural and managerial tone for risk management and security through top-level policies.
- Ensure that personnel with ESP responsibilities have the requisite experience, qualifications, and education.
- Determine risk acceptance, avoidance, and mitigation thresholds that align with strategic and operational goals.
- With senior management, ensure that security risks, threats, and vulnerabilities are regularly assessed and reviewed by using accepted methodologies and best practices.
- Oversee the development and regular review of a risk management plan (RMP) that addresses security risks.
- Exercise oversight of key ESP activities, including
 - development of the Enterprise Security Strategy (ESS)
 - categorization of digital assets
 - selection of controls
 - identification of key performance indicators
 - development and testing of core ESP plans (incident response, crisis communications, business continuity and disaster recovery (BC/DR) and training and implementation).
- Review and approve the enterprise security plan and security business case and funding requirements.
- Ensure formal reviews of the ESP are conducted on a regular basis and that identified weaknesses are addressed.
- Obtain board approval of the RMP and security budget.

BRC Composition

The BRC shall be comprised of seven³⁷ members. Four of the members shall be independent, non-executive directors with experience in risk management, enterprise security, establishing cultures and instilling expectations of compliance, and information technology management.

The BRC shall be comprised of three executive directors:

- Chief executive officer (CEO) or chief operating officer (COO)
- Chief financial officer (CFO)
- Chief risk officer (CRO) or chief security officer (CSO)³⁸

³⁷ The intent is to eliminate tied votes and ensure that independent directors outnumber non-independent directors.

Artifacts Produced by the BRC

The BRC has responsibility for ensuring that the following artifacts are produced from activities related to its goals and objectives:

- BRC mission, goals, objectives, and composition
- X-team mission, goals, and objectives
- Organizational chart depicting ESP lines of authority
- Roles and responsibilities for the ESP
- Top-level ESP policies
- Board-approved budget for the ESP

³⁸ This presumes that the CRO or CSO role includes responsibility for information security. If this is not the case, the chief information security officer is a required member of the BRC.

Appendix B: Cross-Organizational Team (X-Team): Mission, Goals, Objectives, and Composition

Scope

This sample artifact describes the cross-organizational team (X-team) mission, goals, objectives, and composition as identified in Chapter 2, “Defining an Effective Enterprise Security Program,” Table 2, and Chapter 3, “Enterprise Security Governance Activities.”

X-Team Mission

The mission of the cross-organizational team (X-team) is

- to develop, coordinate, and sustain the organization’s enterprise security program (ESP)
- to fulfill the need for an enterprise-wide perspective in
 - coordinating and responding to security risk issues and incidents
 - developing, implementing, and maintaining the organization’s risk management plan (RMP), enterprise security strategy (ESS), and enterprise security plan

X-Team Goals

In carrying out its mission, the X-team shall achieve the following goals:

- Coordinate and communicate security risk issues to ensure they receive enterprise attention as well as adequate and timely responses throughout the organization.
- Ensure that the enterprise security program (ESP) is an active, current, and sustained program, reflected in day-to-day roles, responsibilities, and business processes.
- Facilitate and support the development, implementation, and maintenance of the organization’s risk management plan (RMP), enterprise security strategy (ESS), and enterprise security plan (including supporting plans, such as incident response and disaster recovery) through participation in specified activities.
- Manage the security of digital assets³⁹ in alignment with the RMP, ESS, and enterprise security plan.

X-Team Objectives

The X-team shall accomplish the following objectives in meeting these goals:

- Serve as a central coordination and response point by meeting no less than monthly to discuss security issues and monitor progress on ESP tasks.

³⁹ Digital assets include networks, information, and applications, and their grouping into systems.

- Develop and maintain a comprehensive inventory of systems, including system descriptions, ownership, and custody of assets.
- Identify and maintain a table of authorities for compliance requirements and mappings of assets to the table.
- Map data flows across jurisdictions.
- Map corresponding cybercrime and breach compliance laws to the data flows.
- Conduct security threat and risk self-assessments annually and formal assessments every third year.
- Provide security input to the risk management plan.
- Develop an enterprise security strategy and enterprise security plan for board risk committee (BRC) approval.
- Categorize assets by levels of risk as well as magnitude of harm and impact.
- Determine, review, and update security controls, key performance indicators, and metrics.
- Develop and update supporting plans for the enterprise security plan, including incident response, business continuity/disaster recovery, and crisis communication plans.
- Develop, update, and verify third party and vendor security requirements.
- Develop and update security policies and procedures.
- Develop and update security system architecture plan.
- Develop and update ESP implementation and training plans.
- Monitor and enforce RMP, ESS, and ESP policies and procedures.
- Test and evaluate system controls.
- Identify system weaknesses and plans of action and milestones (POAMs).
- Conduct formal annual reviews of the ESP.

X-Team Composition

The X-team shall be chaired by the chief security officer (CSO) and be comprised of the following additional personnel:

- chief information security officer (CISO) (if this role is separate from the CSO)
- chief risk officer (CRO)
- chief privacy officer (CPO)
- chief information officer (CIO)
- chief financial officer (CFO)
- general counsel (GC)
- business line executives (BLEs)
- vice president of human resources (HR)
- vice president of public relations (PR)

Appendix C: Roles and Responsibilities for an Enterprise Security Program

Scope

This sample artifact describes the leadership roles and responsibilities for the development, implementation, and sustainment of an enterprise security program (ESP), as identified in Chapter 2, “Defining an Effective Enterprise Security Program,” Table 2 and Chapter 3, “Enterprise Security Governance Activities.”

Introduction

The board risk committee (BRC) has responsibility for assigning top-level ESP roles and responsibilities. These include the chief executive officer (CEO), chief operating officer (COO), and members of the cross-organizational ESP team (X-team).

X-team members include the

- chief security officer (CSO),⁴⁰ chair of the X-team
- chief privacy officer (CPO)
- chief information officer (CIO)
- chief financial officer (CFO)
- general counsel (GC)
- business line executives (BLE)
- vice president of human resources (HR)
- vice president of public relations (PR)

In addition to the X-team, business managers (BM), operational personnel (OP), asset owners (AO), and certification authorities (CA) assist in the activities required to develop and sustain an ESP.

The responsibilities assigned to each role are intended to ensure greater accountability through segregation of duties (SOD) and to protect against fraud, malicious acts, and unintended consequences.

⁴⁰ Some organizations have both a CSO and a chief information security officer (CISO), with a separation of duties between facilities and personnel security and information technology (IT) security. As organizations realize, however, that the security of their physical facilities, processes, and personnel is impacted by IT systems and devices, and vice versa, they are integrating the CISO and CSO responsibilities into either a consolidated CSO position or into the chief risk officer (CRO) role [ITCI 06]. As used here, the term CSO encompasses the CISO, although both roles could be subsumed by the CRO. Alternatively, if an organization has both a CSO and CRO, they both participate in the development and sustainment of the ESP, with the CSO taking the lead in implementing the security requirements of the risk management plan, with oversight by the CRO.

Some responsibilities may be shared, requiring special controls, policies and procedures, and careful coordination. Below, we describe specific roles and responsibilities, followed by the name of the artifact that results from executing a given responsibility. Detailed security responsibilities for X-team personnel, business managers (BM), operational personnel (OP), and certification agents (CA) are determined by the CSO with oversight by the BRC. Security responsibilities set by the BRC and CSO help create a culture of security within the organization. They are to be taken seriously. The security responsibilities described here should be included in job descriptions and reviewed as part of performance evaluations.

Roles and Responsibilities

Each role description presents three categories of responsibilities — single, shared, and supporting.

Chief Security Officer (CSO)

CSO Responsibilities

- The CSO has overall responsibility for the ESP and chairs the X-team. The CSO has direct responsibility for leading and guiding the following activities:
- Develop and maintain an inventory of digital assets, with input and assistance from the BLEs, CIO, BM, and AO. Artifact: Inventory of Assets and Systems
- Designate detailed security responsibilities and SOD. Artifact: Detailed Security Responsibilities
- Conduct threat, vulnerability, and risk assessments, including system certification and accreditations, with active assistance from the BLE, BM, OP, and CA. Artifacts: System Risk Assessments
- Develop and update security inputs to the risk management plan, with assistance from the CPO, CIO, and GC. Artifact: Security Inputs to Risk Management Plan
- Develop and update the organization's enterprise security strategy (ESS), with assistance from the CPO. Artifact: Enterprise Security Strategy
- Determine and update necessary controls and ensure they are documented in the ESP. The CSO is assisted in this effort by the CPO, BLE, GC, and BM. Artifact: Assignment of Controls (by system)
- Determine and update key performance indicators and metrics and ensure they are documented in the ESP. The CSO is assisted in this effort by the BLE, CIO, BM, and OP. Artifact: Key Performance Indicators and Metrics
- Identify and maintain a list of security best practices and standards used by the organization, with assistance from the CIO and CPO. Report on the implementation of best practices and standards and map them to controls and metrics. Artifacts: Listing of Approved Best Practices and Standards; Report on Implementation of Best Practices and Standards; Mapping of Best Practices and Standards to Controls and Metrics

- Determine asset-specific security configuration settings. Artifact: Asset Security Configuration Settings
- Develop, update, and test the organization's incident response plan, with assistance from the BLE, CIO, GC, and PR. Test the incident response plan and report on the results. Produce quarterly reports on incidents. Artifacts: Incident Response Plan; Incident Response Plan Test Report; Incident Response Reports
- Develop and update the organization's enterprise security plan. Obtain BRC approval of the ESP. Artifacts: Enterprise Security Plan; ESP Security Update Report
- Develop and update security policies and procedures, with assistance from the CPO, BLE, HR, GC, PR, BM, OP, AO. Artifacts: Security Policies and Procedures
- Develop and update the security system architecture plan, with assistance from the CIO. Artifact: Security System Architecture Plan
- Develop and update the ESP implementation and training plan, with assistance from the CPO, HR, BLE, PR, CIO, GC, BM, AO, and OP. Artifacts: Implementation Plan and Report of Results
- Develop training modules, with assistance from BLE, BM, and OP. Artifacts: Training Modules
- Develop a training plan and schedule, with assistance from the BLE. Artifact: Training Plan and Schedule
- Maintain a record of training, with assistance from HR. Artifact: Record of Training
- Test and evaluate system controls, policies, and procedures (this can be part of a certification and accreditation process), with assistance from the BLE, BM, and CA. Artifact: Testing and Evaluation Report of Controls, Metrics, Policies, and Procedures
- Conduct a formal review of the ESP, with the assistance of the X-team. Artifact: Annual ESP Report

CSO Shared Responsibilities

The CSO shares responsibility with

- the BLE in developing and updating system descriptions. The BLE has responsibility for developing the system descriptions and keeping them current. The CSO has responsibility for ensuring that all required information is collected and entered in the ESP documentation.
- the BLE in establishing and updating ownership and custody of assets. The BLE is responsible for determining ownership and custody of the assets and keeping this information current. The CSO is responsible for gathering this information and recording it in the ESP documentation. Artifact: Ownership and Custody of Assets.
- the GC and CPO for determining and updating compliance requirements. The GC is responsible for developing and maintaining the table of authorities. The CPO is responsible for ensuring that all applicable privacy laws and Regulations have been identified and entered on the table of authorities. The CSO is responsible for ensuring that all applicable security laws and regulations have been identified and entered on the table of authorities.

The CSO is responsible for ensuring the table of authorities is entered into the ESP documentation and kept up to date.

- the GC and CPO in mapping assets to the table of authorities. The CSO and CPO are responsible for ensuring that all assets are included in the mapping exercise.
- the BLE in categorizing assets by levels of risk and magnitude of harm, with assistance from the CPO, GC, and BM. The CSO leads the categorization exercise, and the BLE provides critical input regarding the risk the asset poses to the organization and the magnitude of harm that could result from disruption or loss of the asset. Artifact: Categorization of Assets.
- the CIO and BLE in developing, updating, and testing a business continuity and disaster recovery (BC/DR) Plan, with assistance from BM and OP. The CSO, CIO, and BLE each bring unique knowledge to the development and maintenance of a BC/DR plan. The CSO has the lead responsibility for gathering the requirements and producing the plan and test report. Artifacts: BC/DR Plan; BC/DR Test Report.
- the CIO in developing, updating, and verifying third party and vendor security requirements for business continuity and disaster recovery, incident response (IR), and crisis communications (CC), with input from the BLE. The CSO is responsible for gathering the information and preparing associated reports. Artifacts: Third Party and Vendor Requirements for BC/DR, IR, and CC; Third Party and Vendor Requirements Verification Report.
- the CIO in developing and updating change management plans. The CIO provides input pertaining to operational integrity and availability, and the CSO provides input from the security perspective. Artifacts: Change Management Plan; Change Management Logs.
- the GC and HR in monitoring and enforcing security policies and procedures, with assistance from the CPO, BLE, and BM. The GC provides input about legal considerations and monitoring restrictions and helps enforce policies and procedures. The HR incorporates monitoring and enforcement policies and procedures into personnel policies and guidelines, and helps enforce policies and procedures. Artifacts: Monitoring and Enforcement Reports.
- the CA in identifying system weaknesses and executing a corrective action process, with assistance from the BLE and BM. The CSO has the responsibility to ensure the corrective Plan of Action and Milestones is completed and appropriate documentation entered in the ESP.
- the CFO in determining the security business case, including return on investment calculations and funding requirements for the ESP. Artifact: ESP Security Investment Requirements and ROI Analysis.

CSO Assistance Responsibilities

The CSO assists

- the CPO in mapping and analyzing data flows.
- the GC in mapping cybercrime and security breach notification laws and cross-border cooperation with law enforcement to data flows.
- the CPO in conducting privacy impact assessments and privacy audits.

- the PR in developing, updating, and testing the organization’s crisis communications plan, and in producing the crisis communications plan test report and quarterly crisis communications reports.

Chief Privacy Officer (CPO)

CPO Responsibilities

The CPO has direct responsibility for

- mapping and analyzing data flows, with the assistance from the CSO, BM, and AO. Artifact: Mapping and Analysis of Data Flows
- conducting privacy impact assessments and privacy audits, with assistance from the GC and CSO. Artifacts: Privacy Impact Assessments; Privacy Audit Reports

CPO Shared Responsibilities

The CPO shares responsibility with

- the GC and CSO for determining and updating compliance requirements. The GC is responsible for developing and maintaining the table of authorities. The CPO is responsible for ensuring that all applicable privacy laws and regulations have been identified and entered on the table of authorities. The CSO is responsible for ensuring that all applicable security laws and regulations have been identified and entered on the table of authorities. The CSO is responsible for ensuring the table of authorities is entered into the ESP documentation and kept up-to-date.
- the CSO and GC in mapping assets to the table of authorities. The CSO and CPO are responsible for ensuring that all assets are included in the mapping exercise.

CPO Assistance Responsibilities

The CPO assists

- the GC in mapping cybercrime and security breach notification laws and cross-border cooperation with law enforcement to data flows.
- the CSO in developing and updating security inputs to the risk management plan.
- the CSO in developing and updating the organization’s enterprise security strategy.
- the CSO and BLE in categorizing assets by levels of risk and magnitude of harm.
- the CSO in determining and updating necessary controls.
- the CSO in identifying and maintaining a list of best practices and standards used by the organization.
- the CSO in developing and updating security policies and procedures. The CPO must ensure privacy considerations are taken into account in the policies and procedures.
- the CSO in developing and updating ESP implementation and training plans.
- the CSO, GC, and HR in monitoring and enforcing security policies and procedures.
- the CSO in conducting a formal review of the ESP.

Chief Information Officer (CIO)

CIO Shared Responsibilities

The CIO shares responsibility with

- the CSO and BLE in developing, updating, and testing a business continuity and disaster recovery (BC/DR) plan, with assistance from BM and OP. The CSO, CIO, and BLE each bring specific knowledge to the development and maintenance of a BC/DR plan.
- the CSO in developing, updating, and verifying third party and vendor security requirements for business continuity and disaster recovery, incident response (IR), and crisis communications (CC), with input from the BLE. The CIO provides input regarding network and application requirements and other aspects of IT asset management. The CSO is responsible for gathering the information and preparing associated reports.
- the CSO in developing and updating change management plans. The CIO provides input pertaining to operational integrity and availability, and the CSO provides input from the security perspective.

CIO Assistance Responsibilities

The CIO assists

- the CSO in the development and maintenance of an inventory of digital assets.
- the BLE and CSO in developing and updating system descriptions.
- the CSO and BLE in establishing and updating ownership and custody of assets.
- the CSO in developing and updating security inputs to the risk management plan.
- the CSO in determining and updating key performance indicators and metrics.
- the CSO in identifying and maintaining a list of best practices and standards utilized by the organization.
- the CSO in developing, updating, and testing the organization's incident response plan.
- the PR in developing, updating, and testing the organization's crisis communications plan, and in producing the crisis communications plan test report and quarterly crisis communications reports.
- the CSO in developing and updating security system architecture plan.
- the CSO in developing and updating ESP implementation and training plan.
- the CSO in conducting a formal review of the ESP.

Chief Financial Officer (CFO)

CFO Shared Responsibilities

The CFO

- shares responsibility with the CSO in determining the security business case, including return on investment calculations and funding requirements for the ESP.

CFO Assistance Responsibilities

The CFO assists

- the CSO in conducting a formal review of the ESP.

General Counsel (GC)

GC Responsibilities

The GC has direct responsibility for

- mapping cybercrime and security breach notification laws and cross-border cooperation with law enforcement to data flows, with assistance from the CSO, CPO, and BLE. Artifact: Mapping of Cybercrime and Notification Laws and Cross-Border Cooperation

GC Shared Responsibilities

The GC shares responsibility with

- the CSO and CPO for determining and updating compliance requirements. The GC is responsible for developing and maintaining the table of authorities. The CPO is responsible for ensuring that all applicable privacy laws and regulations have been identified and entered on the table of authorities. The CSO is responsible for ensuring that all applicable security laws and regulations have been identified and entered on the table of authorities. The CSO is responsible for ensuring the table of authorities is entered into the ESP documentation and kept up-to-date. Artifact: Table of Authorities
- the CSO and CPO in mapping assets to the table of authorities. The CSO and CPO are responsible for ensuring that all assets are included in the mapping exercise. Artifact: Mapping of Assets and Authorities
- the CSO and HR in monitoring and enforcing security policies and procedures, with assistance from the CPO, BLE, and BM. The GC provides input regarding legal considerations and monitoring restrictions, and helps enforce policies and procedures.
- The HR incorporates monitoring and enforcement policies and procedures into personnel policies and guidelines, and helps enforce policies and procedures.

GC Assistance Responsibilities

The GC assists

- the CPO in conducting privacy impact assessments and privacy audits.
- the CSO in developing and updating security inputs to the risk management plan.

- the CSO and BLE in categorizing assets by levels of risk and magnitude of harm.
- the CSO in determining and updating necessary controls.
- the CSO in developing, updating, and testing the organization's incident response plan.
- the CSO in developing and updating security policies and procedures. The GC must ensure that legal compliance and liability considerations are included in security policies and procedures.
- the CSO in developing and updating ESP implementation and training plans.
- the CSO in conducting a formal review of the ESP.

Business Line Executives (BLE)

BLE Responsibilities

The BLE has direct responsibility for

- determining operational criteria, with input from the BM. Artifact: Operational Criteria
- issuing an authority to operate (ATO) or interim authority to operate (IATO) for each system or denying a system authority to operate. Artifact: Accreditation Decision Letter

BLE Shared Responsibilities

The BLE shares responsibility with

- the CSO in developing and updating system descriptions. The BLE has responsibility for developing the system descriptions and keeping them current. The CSO has responsibility for ensuring that all required information is collected and entered in the ESP documentation. Artifact: System Descriptions
- the CSO in establishing and updating ownership and custody of assets. The BLE is responsible for determining ownership and custody of the assets and keeping this information current. The CSO is responsible for gathering this information and recording it in the ESP documentation.
- the CSO in categorizing assets by levels of risk and magnitude of harm, with assistance from the CPO, GC, and BM. The CSO leads the categorization exercise, and the BLE provides critical input regarding the risk the asset poses to the organization and the magnitude of harm that could result from disruption or loss of the asset.
- the CSO and CIO in developing, updating, and testing a business continuity and disaster recovery (BC/DR) plan, with assistance from BM and OP. The CSO, CIO, and BLE each bring specific knowledge to the development and maintenance of a BC/DR plan.

BLE Assistance Responsibilities

The BLE assists

- the CSO in the development and maintenance of an inventory of digital assets.
- the GC, CPO, and CSO in determining and updating compliance requirements on the table of authorities.

- the GC, CSO, and CPO in mapping assets to the table of authorities.
- the GC in mapping cybercrime and security breach notification laws and cross-border cooperation with law enforcement to data flows.
- the CSO in conducting threat, vulnerability, and risk assessments, including system certification and accreditations.
- the CSO in determining and updating necessary controls.
- the CSO in determining key performance indicators and metrics.
- the CSO in developing, updating, and testing the organization's incident response plan .
- the PR in developing, updating, and testing the organization's crisis communications plan, and in producing the crisis communications plan test report.
- the CSO and CIO in developing, updating, and verifying third party and vendor security requirements for business continuity and disaster recovery, incident response (IR), and crisis communications (CC).
- the CSO in developing and updating security policies and procedures.
- the CSO in developing and updating ESP implementation and training plans.
- the CSO in developing training modules to ensure business considerations and requirements are included.
- the CSO in developing the training plan and schedule.
- the CSO, GC, and HR in monitoring and enforcing security policies and procedures.
- the CSO in testing and evaluating system controls, policies and procedures (this can be part of a certification and accreditation process).
- the CA in identifying system weaknesses and executing a corrective action process.
- the CSO in conducting a formal review of the ESP.

Human Resources (HR)

HR Shared Responsibilities

The HR shares responsibility with

- the CSO and GC in monitoring and enforcing security policies and procedures, with assistance from the CPO, BLE, and BM. The GC provides input regarding legal considerations and monitoring restrictions and assists with enforcement of policies and procedures. The HR incorporates monitoring and enforcement policies and procedures into personnel policies and guidelines, and helps enforce policies and procedures.

HR Assistance Responsibilities

The HR assists

- the CSO in developing and updating security policies and procedures. The HR must ensure that compliance with security policies and procedures is embedded in job descriptions and performance evaluations.
- the CSO in developing and updating ESP implementation and training plans.
- the CSO in maintaining a record of training.
- the CSO in conducting a formal review of the ESP.

Public Relations (PR)

PR Responsibilities

The PR has direct responsibility for

- developing, updating, and testing the organization's crisis communications plan, with assistance from the CSO, CIO, and BLE. Testing the crisis communications plan and reporting on the results. Producing quarterly crisis communication reports. Artifacts: Crisis Communications Plan; Crisis Communications Plan Test Report; Crisis Communication Reports

PR Assistance Responsibilities

The PR assists

- the CSO in developing, updating, and testing the organization's incident response plan.
- the CSO in developing and updating security policies and procedures. The PR must ensure that public relations considerations are included in security policies and procedures.
- the CSO in developing and updating ESP implementation and training plans.
- the CSO in conducting a formal review of the ESP.

Business Managers (BM)

BM Assistance Responsibilities

The BM assists

- the CSO in the development and maintenance of an inventory of digital assets.
- the CSO and BLE in developing and updating system descriptions.
- the CSO and BLE in establishing and updating ownership and custody of assets.
- the CPO in mapping and analyzing data flows.
- the CSO in conducting threat, vulnerability, and risk assessments, including system certification and accreditations.
- the BLE in determining operational criteria.
- the CSO and BLE in categorizing assets by levels of risk and magnitude of harm.

- the CSO in determining and updating necessary controls.
- the CSO in determining key performance indicators and metrics.
- the CSO, CIO and BLE in developing, updating, and testing a business continuity and disaster recovery (BC/DR) Plan.
- the CSO in developing and updating security policies and procedures.
- the CSO in developing and updating ESP implementation and training plans.
- the CSO in developing training modules to ensure business considerations and requirements are included.
- the CSO, GC, and HR in monitoring and enforcing security policies and procedures.
- the CSO in testing and evaluating system controls, policies and procedures (this can be part of a certification and accreditation process).
- the CA in identifying system weaknesses and executing a corrective action process.

Operational Personnel (OP)

OP Assistance Responsibilities

The OP assist

- the CSO in conducting threat, vulnerability, and risk assessments, including system certification and accreditations.
- the CSO in determining key performance indicators and metrics.
- the CSO, CIO and BLE in developing, updating, and testing a business continuity and disaster recovery (BC/DR) plan.
- the CSO in developing and updating security policies and procedures.
- the CSO in developing and updating ESP implementation and training plans.
- the CSO in developing training modules to ensure business considerations and requirements are included.

Asset Owners (AO)

AO Assistance Responsibilities

The AO assists

- the CSO in developing and maintaining an inventory of digital assets.
- the CSO and BLE in developing and updating system descriptions.
- the CSO and BLE in establishing and updating ownership and custody of assets.
- the CPO in mapping and analyzing data flows.
- the CSO in developing and updating security policies and procedures.
- the CSO in developing and updating ESP implementation and training plans.

Certification Authority (CA)

CA Shared Responsibilities

The CA shares responsibility with

- the CSO in identifying system weaknesses and executing a corrective action process, with assistance from the BLE and BM. Artifact: System Plan of Action and Milestones

CA Assistance Responsibilities

The CA assists

- the CSO conduct threat, vulnerability, and risk assessments, including system certification and accreditations. Artifact: Certification Letters
- the CSO in testing and evaluating system controls, policies and procedures (this can be part of a certification and accreditation process).

Author Biographies

Jody R. Westby

Drawing upon a unique combination of more than twenty years of technical, legal, policy, and business experience, Ms. Westby provides consulting and legal services to public and private sector clients around the world in the areas of privacy, security, outsourcing risk management, business continuity, and technology compliance issues. She also serves as Adjunct Distinguished Fellow for Carnegie Mellon CyLab.

Prior to forming Global Cyber Risk, Ms. Westby served as senior managing director for PricewaterhouseCoopers (PwC), specializing in outsourcing and cyber security/privacy issues. Before that, she was president of The Work-IT Group; launched In-Q-Tel, an IT venture capital/solutions company for the CIA; served as director of domestic policy for the U.S. Chamber of Commerce; was senior fellow and director of IT studies for the Progress & Freedom Foundation; practiced law with two top-tier New York firms; and spent ten years in the computer industry specializing in database management systems.

Jody is a member of the bars of the District of Columbia, Pennsylvania, and Colorado and serves as chair of the American Bar Association's Privacy and Computer Crime Committee. She is a member of the World Federation of Scientists' Permanent Monitoring Panel on Information Security and represents the ABA on the National Conference of Lawyers and Scientists. She is co-author and editor of four books on privacy, security, cybercrime, and enterprise security programs. She speaks globally and is the author of numerous chapters. B.A., summa cum laude, University of Tulsa; J.D., magna cum laude, Georgetown University Law Center; Order of the Coif.

Julia Allen

Julia Allen is a senior researcher within the CERT Program at the Software Engineering Institute (SEI), a unit of Carnegie Mellon University in Pittsburgh, PA. Allen is engaged in developing and transitioning executive outreach programs in enterprise security and governance.

Prior to this technical assignment, Allen served as acting Director of the SEI for an interim period of 6 months as well as Deputy Director/Chief Operating Officer for 3 years. Her degrees include a B. Sci. in Computer Science (University of Michigan) and an MS in Electrical Engineering (University of Southern California). She is the author of *The CERT Guide to System and Network Security Practices* (Addison-Wesley, June 2001), *Governing for Enterprise Security* (CMU/SEI-2005-TN-023, 2005), and CERT's podcast series: Security for Business Leaders.

Podcast Overview

Included with this document is a CD-ROM containing four podcasts that discuss different aspects of governance as it relates to security as well as an electronic copy of this document. At the date of this publication, these podcasts, and others can be found on the CERT website at the following URL: <http://www.cert.org/podcast/#governing>.

Here is a summary of the podcasts contained on the CD-ROM.

Getting Real About Security Governance

Enterprise security governance is not just a vague idea – it can be achieved by implementing a defined, repeatable process with specific activities.

For an organization that lacks a cohesive enterprise security governance program, establishing one may seem like an overwhelming endeavor. In fact, however, this is not the case. By breaking down enterprise security governance into its component activities, organizations can design and build a security governance program over time, tailoring it to suit their needs.

Toward this goal, Julia Allen, a senior researcher with CERT, has co-authored an implementation guide for enterprise security governance. In this podcast, we discuss that research and how organizations can use it as a framework for establishing effective, sustainable security governance programs.

The Legal Side of Global Security

Business leaders, including legal counsel, need to understand how to tackle complex security issues for a global enterprise.

In this podcast, Jody Westby, CEO of Global Cyber Risk and Chair of the American Bar Association's Privacy and Computer Crime Committee, talks about a range of security-related issues when conducting business in a global marketplace. These include protecting data as it travels across borders, outsourcing operations, understanding jurisdiction differences and protecting client and work-product privilege, and tackling the new roles that legal counsel and business leaders need to fill.

Why Leaders Should Care About Security

Leaders need to be security conscious and to treat adequate security as a non-negotiable requirement of being in business.

Security's days as just a technical issue are done. It is becoming a central concern for leaders at the highest level of many organizations and governments, transcending national borders. Customers are demanding it as worries about privacy and identity theft grow.

Business partners, suppliers, and vendors are requiring it from one another, particularly when providing mutual network and information access. Networked efforts to steal competitive intelligence and engage in extortion are becoming more prevalent. Security breaches are increasingly motivated by financial gain.

This podcast is intended to motivate leaders to pay attention to enterprise and information security, and the risks of not doing so. It introduces two landmark examples of organizations that did not treat adequate security as a high priority. It places security in a governance context and introduces how security can be viewed as a competitive advantage. It discusses creating a culture of security, demonstrating duty of care, and determining who is ultimately responsible for security. It provides some next steps for taking action.

Compliance vs. Buy-In

Integrating security into standard business operating processes and procedures is more effective than treating security as a compliance exercise.

Demonstrating compliance with the increasing number of domestic and international laws and regulations is a daunting undertaking if this is tackled one regulation at a time. Organizations that have implemented a living set of standard operating processes and procedures (SOP) find that a small team can generally trace any new external requirement to their SOP. This typically produces a set of manageable changes, many of which result in minimal to no impact to the rest of the organization.

An SOP typically includes well defined roles and responsibilities, commitments and accountabilities; policies and procedures; business process definitions; controls; regular monitoring and reporting; and training and awareness.

Thus compliance is an outcome of good business practice, not a focus for special task teams or projects.

Acronyms

AO	Asset Owners
APEC	Asia-Pacific Economic Cooperation
ASIS	American Society for Industrial Security
ATO	Authorization To Operate
BAC	Board Audit Committee
BC	Business Continuity
BCR	Binding Corporate Rules
BLE	Business Line Executive
BM	Business Managers
BRC	Board Risk Committee
BSI	British Standards Institute
C&A	Certification & Accreditation
CA	Certification Agent
CAI	Confidentiality, Availability, Integrity
CC	Crisis Communication
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CGTF	Corporate Governance Task Force
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CobIT	Control Objectives for Information and related Technology
CoE	Council of Europe
COO	Chief Operating Officer

CPO	Chief Privacy Officer
CRO	Chief Risk Officer
CSO	Chief Security Officer
DHS	Department of Homeland Security
DP	Data Protection
DR	Disaster Recovery
EA	External Audit
ECPA	Electronic Communications Privacy Act
EEA	Economic Espionage Act
ERM	Enterprise Risk Management
ESP	Enterprise Security Program
ESS	Enterprise Security Strategy
EU	European Union
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FTC	Federal Trade Commission
GC	General Counsel
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
HR	Human Resources
IA	Internal Audit
IATO	Interim Authorization To Operate
IFAC	International Federation of Accountants
IIA	Institute of Internal Auditors
IR	Incident Response

ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISSA	Information Systems Security Association
IT	Information Technology
ITGI	IT Governance Institute
KPI	Key Performance Indicator
MLAT	Mutual Legal Assistance Treaty
NIST	National Institute of Standards and Technology
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OP	Operational Personnel
P6STNI	People, Products, Plants, Processes, Policies, Procedures, Systems, Technologies, Networks, and Information
PDA	Personal Digital Assistant
PIPEDA	Personal Information Protection and Electronics Document Act
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identify Verification
POAM	Plans Of Action and Milestones
PR	Public Relations
RFID	Radio Frequency Identification
RMP	Risk Management Plan
ROI	Return On Investment
RTO	Recovery Time Objectives
SCADA	Supervisory Control And Data Acquisition
SDLC	System Development Life Cycle

SEC	Securities & Exchange Commission
SOD	Segregation Of Duties
SRMP	Security Risk Management Plan
USCCU	U.S. Cyber Consequences Unit
VOIP	Voice Over Internet Protocol
X-team	Cross organizational ESP team

Glossary

Accreditation The official management decision given by a senior officer or BLE to authorize the operation of an information system and to explicitly accept the risk to the organization's operations, assets, or personnel based on the implementation of an agreed-upon set of controls. By accrediting an information system, senior management accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the organization if a breach of security occurs.

Authorization to operate See accreditation.

Availability Timely, reliable access to data and information services for authorized users [CNSS 01].

Boundary (system) Determined by the IT resources assigned to a particular system [Swanson 06]. System boundaries are usually determined during the inventory process.

Certification A detailed security review of a system that results in the information and supporting evidence (artifacts) needed for security accreditation.

Confidentiality Assurance that information is not disclosed to unauthorized individuals, processes, or devices [CNSS 01].

Convergence The identification of security risks and interdependencies between business functions and processes within the enterprise and the development of managed business process solutions to address those risks and interdependencies [AESRM 05].

Cybercrime Convention See the Council of Europe Convention on Cybercrime description at <http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm>.

Data flows When data is transmitted from one user to another or from one physical location to another, it is called a data flow, (i.e., the data flows from one person or place to another). With respect to location, data could flow from one server to another or from one state or country to another. Such flows of data raise numerous security considerations, such as compliance with different laws from jurisdiction to jurisdiction; the policies and procedures required to ensure that security requirements are passed from one user or location to the next; and the technical software and tools that must follow the data to ensure security is effectively deployed and maintained.

Enterprise governance The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization's resources are used responsibly [IFAC 04].

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); Treating adequate security as a non-negotiable requirement of being in business [Allen 05].

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; and “ provide assignment of responsibility all in an effort to manage risk [Bowen 06].

Integrity (data integrity) Data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. (integrity) protection against unauthorized modification or destruction of information [CNSS 01].

IT governance An integral part of enterprise governance. It consists of the leadership and organizational structures and processes that ensure that the organization’s IT sustains and extends the organization’s strategies and objectives [ITGI 03].

Key performance indicator Financial and non-financial metrics used to quantify objectives to reflect strategic performance of an organization.
http://en.wikipedia.org/wiki/Key_performance_indicators

Letter rogatory a formal request from a court in one country to “the appropriate judicial authorities” in another country requesting compulsion of testimony or documentary or other evidence or effect service of process.
http://en.wikipedia.org/wiki/Letter_rogatory

Operational criteria Determined by business line executives (BLEs) and include the baseline IT requirements for the operation of their business unit, such as network availability, interconnectivity requirements, use of portable devices, and number of users requiring software licenses. Operational criteria can also include business continuity and disaster recovery parameters and details regarding the working environment, such as heavy traffic flow within the operational area, physical layout considerations, and extreme climate conditions.

Resilience an organization’s ability to adaptively respond to disruptive events and tolerate being affected by them.

Risk “a function of the likelihood of a given threat-source’s exercising a particular vulnerability, and the resulting impact of that adverse event on the organization” [Stoneburner 02].

System “a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information” [Ross 04]. Information resources include networks, applications, and data. C&As are performed on systems, and security requirements apply throughout the system development life cycle (SDLC).

System architecture The technical network and system components (hardware and firmware), operating platforms and application software, and other hardware or software components used within the IT environment. System architecture differs from “enterprise architecture,” which describes the alignment between business functions and IT assets.

System description Includes the purpose of the system, the information resources (or assets) that comprise it, how the assets are used, the asset owners and custodians, any special protections required, etc. [Ross 04].

Table of Authorities Listing of all applicable laws, regulations, directives, contracts, and other legal requirements applicable to the organization’s assets and systems.

Top-level policies Broad statements that support the risk objectives of the organization that pertain to security. Top-level security governance policies establish the expected behavior and cultural norms that are required to sustain an effective enterprise security program. Top-level security management policies govern operations and the use of technology.

References

[Acuff 00]

Acuff, Jr., A. Marshall. "Information Security Impacting Securities Valuations: Information Technology and the Internet Changing the Face of Business," Institute of Internal Auditors. <http://www.theiia.org/ITAudit/index.cfm?act=itaudit.archive&fid=143> (2000).

[AESRM 05]

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

[Allen 05]

Allen, Julia. "Governing for Enterprise Security." (CMU/SEI-2005-TN-023). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, June 2005. <http://www.sei.cmu.edu/publications/documents/05.reports/05tn023.html>.

[Allen 06a]

Allen, Julia. "Why Leaders Should Care About Security." CERT Podcast Series: Security for Business Leaders, 2006-2007. <http://www.cert.org/podcast/show/leaders.html>.

[Allen 06b]

Allen, Julia. "Security Is Not Just a Technical Issue." Build Security In web site, Department of Homeland Security, October 2006. <https://buildsecurityin.us-cert.gov/daisy/bsi/chapters/best-practices/management/563.html>.

[Allen 06c]

Allen, Julia. "Framing Security as a Governance and Management Concern: Risks and Opportunities." Department of Homeland Security, Build Security In web site, October 2006. <https://buildsecurityin.us-cert.gov/daisy/bsi/chapters/best-practices/management/565.html>.

[Allen 06d]

Allen, Julia. "Navigating the Security Practice Landscape." Department of Homeland Security, Build Security In web site, October 2006. <https://buildsecurityin.us-cert.gov/daisy/bsi/chapters/best-practices/deployment/582.html>.

[Allen 06e]

Allen, Julia. "Plan, Do, Check, Act." Department of Homeland Security, Build Security In web site, November 2006. <https://buildsecurityin.us-cert.gov/daisy/bsi/chapters/best-practices/deployment/574.html>.

[APEC 05]

APEC Privacy Framework. Asia-Pacific Economic Cooperation, 2005.
http://www.apec.org/apec/news___media/2004_media_releases/201104_apecminsendorsepri_vacyfrmwk.html.

[Baker 06]

Global Privacy Handbook, Baker & McKenzie, 2006.

[Barker 04a]

Barker, William C. Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, (NIST Special Publication 800-60, Version 2). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, June 2004.
<http://csrc.nist.gov/publications/nistpubs/index.html>.

[Barker 04b]

Barker, William C., et al. Volume II: Appendixes to Guide for Mapping Types of Information and Information Systems to Security Categories, (NIST Special Publication 800-60, Version 2). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, June 2004.
<http://csrc.nist.gov/publications/nistpubs/index.html>.

[Bolton 03]

Bolton, Joshua B. "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 26, 2003.
<http://www.whitehouse.gov/omb/memoranda/m03-22.html#a>.

[Bowen 06]

Bowen, Pauline, et al. 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, October 2006.
<http://csrc.nist.gov/publications/nistpubs/index.html>.

[Braithwaite 02]

Braithwaite, Timothy. *Securing E-Business Systems: A Guide for Managers and Executives*. John Wiley & Sons, Inc., 2002.

[BRT 05]

Business Roundtable. Principles of Corporate Governance 2005, Business Roundtable, November 2005.
<http://www.businessroundtable.org/pdf/CorporateGovPrinciples.pdf> (pdf).

[BSA 03]

Business Software Alliance. "Information Security Governance: Toward a Framework for Action." October 2003.

<http://www.bsa.org/country/Research%20and%20Statistics/~media/BD05BC8FF0F04CBD9D76460B4BED0E67.ashx>.

[BSI 06]

Business continuity management - Part 1: Code of Practice, (BS 25999-1:2006). London, United Kingdom, British Standards Institute, November 2006. Ordering information available at <http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030157563>.

[Caralli 04]

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

<http://www.sei.cmu.edu/publications/documents/04.reports/04tn046.html>.

[Cashell 04]

Cashell, Brian, et al. "The Economic Impact of Cyber-Attacks." Congressional Research Service, April 2004.

http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf (pdf).

[CGTF 04]

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

http://www.cyberpartnership.org/InfoSecGov4_04.pdf (pdf).

[Chew 06]

Elizabeth, Chew, et al. Guide for Developing Performance Metrics for Information Security, Initial Public Draft (NIST Special Publication 800-80). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, May 2006.

<http://csrc.nist.gov/publications/nistpubs/index.html>.

[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.

<http://www.educase.edu/LibraryDetailPage/666&ID=CSD3661>.

[COC 06a]

Council on Competitiveness. Achieving Competitiveness and Security: Financial Services Sector Study, Council on Competitiveness, 2006.

<http://www.compete-resilience.org/index.php?mp=5&doc=15>.

[COC 6b]

Council on Competitiveness. "The Value of Resilience." Council on Competitiveness, Oct. 13, 2006.

<http://www.compete-resilience.org/index.php?mp=5&doc=56>.

[CNSS 01]

Committee on National Security Systems. National Information Assurance Glossary, CNSS Instruction No. 4009, National Security Agency, June 2006.

http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.

[DHS 06]

Privacy Impact Assessments: Official Guidance. U.S. Department of Homeland Security, The Privacy Office, March 2006.

http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_march_v5.pdf (pdf).

[EPIC 06]

Privacy & Human Rights: An International Survey of Privacy Laws and Developments. Electronic Privacy Information Center and Privacy International, 2006. Ordering information available at

<http://www.powells.com/biblio/1893044254?&PID=24075>.

[FIPS 04]

Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards Publication (FIPS PUB 199). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, February 2004.

<http://csrc.nist.gov/publications/fips/>.

[FISMA 02]

Federal Information Security Management Act, Title III of E-Government Act of 2002, Pub. Law 107-347.

<http://csrc.nist.gov/policies/FISMA-final.pdf>.

[FTC 02a]

In re Eli Lilly and Co., File No. 012 3214, Docket No. C-4047.

<http://www.ftc.gov/os/2002/01/lillycmp.pdf>.

[FTC 02b]

In re Eli Lilly and Co., Agreement Containing Consent Order, FTC No. 0123214, Jan 18, 2002.

<http://www.ftc.gov/os/2002/01/lillyagree.pdf> (consent order accorded final approval on May 10, 2002).

[GAO 99]

U.S. General Accounting Office. Federal Information Systems Control Audit Manual. U.S. General Accounting Office, Accounting and Information Management Division, GAO/AIMD-12.19.6, January 1999. <http://www.gao.gov/special.pubs/ai12.19.6.pdf>.

[Gordon 06]

Gordon, Lawrence & Loeb, Martin. *Managing Cybersecurity Resources: A Cost-Benefit Analysis*, McGraw-Hill, 2006.

[Grance 04a]

Grance, Tim, et al. *Computer Security Incident Handling Guide* (NIST Special Publication 800-61). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, January 2004.
<http://csrc.nist.gov/publications/nistpubs/index.html>.

[Grance 04b]

Grance, Tim, et al. *Security Considerations in the Information System Development Life Cycle* (NIST Special Publication 800-64 Rev. 1). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, June 2004.
<http://csrc.nist.gov/publications/nistpubs/index.html>.

[Kim 06]

Kim, Gene, et al. "Prioritizing IT Controls for Effective, Measurable Security." Department of Homeland Security, Build Security In web site, October 2006. <https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/deployment/577.html>.

[Harris 06]

Harris, Shon. "Introduction to Security Governance." SearchSecurity.com, August 22, 2006.
http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1210565,00.html

[Hash 05]

Hash, Joan, et al. *Integrating IT Security into the Capital Planning and Investment Control Process* (NIST Special Publication 800-65). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, January 2005.
<http://csrc.nist.gov/publications/nistpubs/index.html>.

[IFAC 04]

International Federation of Accountants. "Enterprise Governance: Getting the Balance Right," International Federation of Accountants, Professional Accountants in Business Committee, 2004.
<http://www.ifac.org/Members/DownLoads/EnterpriseGovernance.pdf> (pdf).

[IIA 01]

Institute of Internal Auditors. "Information Security Governance: What Directors Need to Know." Institute of Internal Auditors, Critical Infrastructure Assurance Project, 2001.
<http://www.theiia.org/download.cfm?file=7382>.

[ISACA 05a]

Convergence of Enterprise Security Organizations. Information Systems Audit and Control Association, November 8, 2005.
<http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=22607>.

[ISACA 05b]

Segregation of Duties Within Information Systems. Information Systems Audit and Control Association, Certified Information Systems Auditor (CISA) Review Manual 2005 at 88-91. http://www.isaca.org/Content/ContentGroups/Certification3/CRM_Segregation_of_Duties.pdf (pdf).

[ISO 05a]

International Organization for Standardization. Information technology - Security techniques - Code of practice for information security management. ISO/IEC 17799:2005(E), Second edition, June 15, 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.

[ITCI 06]

IT Audit Checklist: Risk Management. IT Compliance Institute, 2006. <http://www.itcinstitute.com/display.aspx?id=2499>.

[ITGI 03]

IT Governance Institute. Board Briefing on IT Governance, IT Governance Institute, 2003. http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=6658&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

[ITGI 05a]

Aligning CobiT, ITIL and ISO 17799 for Business Benefit: Management and Summary. IT Governance Institute, Office of Government Commerce, the IT service Management Forum, 2005. <http://www.itgovernance.co.uk/files/ITIL-COBiT-ISO17799JointFramework.pdf>.

[ITGI 05b]

Information Technology Governance Institute. COBIT 4.0 Control Objectives for Information and related Technology. ITGI, 2005. <http://www.itgi.org> and <http://www.isaca.org>.

[ITGI 06]

Information Technology Governance Institute. Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition. ITGI, 2006. http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=24384.

[NIST 05]

Revised NIST SP 800-26 System Questionnaire with NIST SP 800-53 References and Associated Security Control Mappings, (NIST SP 800-26Q). Gaithersburg, MD: Computer

Security Division, Information Technology Laboratory, National Institute of Standards and Technology, April 2005.
<http://csrc.nist.gov/publications/nistpubs/index.html>.

[Ross 04]

Ross, Ron, et al. Guide for the Security Certification and Accreditation of Federal Information Systems, (NIST Special Publication 800-37). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, May 2004.
<http://csrc.nist.gov/publications/nistpubs/index.html>.

[Ross 05a]

Ross, Ron, et al. Recommended Security Controls for Federal Information Systems, Draft (NIST Special Publication 800-53, Revision 1). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, December 2006.
<http://csrc.nist.gov/publications/nistpubs/index.html>.

[Ross 05b]

Ross, Ron, et al. Guide to Assessing the Security Controls in Federal Information Systems, 2nd Public Draft (NIST Special Publication 800-53A). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, April 2006.
<http://csrc.nist.gov/publications/drafts.html>.

[Ross 06]

Ross, Ron. Managing Enterprise Risk in Today's World of Sophisticated Threats: A Framework for Developing Broad-Based, Cost-Effective Information Security Programs, National Institute of Standards & Technology, 2006.
<http://csrc.nist.gov/sec-cert/rmf-sz.pdf> (pdf).

[Smedinghoff 06]

Smedinghoff, Thomas J. "Where We're Headed-New Developments and Trends in the Law of Information Security." Wildman Harrold, Nov. 2006.
<http://www.wildmanharrold.com/index.cfm?fa=news.pubArticle&aid=5072F372-BDB9-4A10-554DF441B19981D7>.

[Steven 06]

Steven, John. "Adopting an Enterprise Software Security Framework." IEEE Security & Privacy, IEEE Computer Society, March/April 2006. <https://buildsecurityin.us-cert.gov/daisy/bsi/resources/published/series/bsi-ieee/568.html>.

[Stoneburner 02]

Stoneburner, Gary, et al. Risk Management Guide for Information Technology Systems (Special Publication 800-30). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, July 2002.
<http://csrc.nist.gov/publications/nistpubs/index.html>.

[Swanson 01]

Swanson, Marianne. Security Self-Assessment Guide for Information Technology Systems (NIST Special Publication 800-26). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, November 2001.

<http://csrc.nist.gov/publications/nistpubs/index.html>.

[Swanson 03]

Swanson, Marianne, et al. Security Metrics Guide for Information Technology Systems (NIST Special Publication 800-55). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, July 2003.

<http://csrc.nist.gov/publications/nistpubs/index.html>.

[Swanson 06]

Swanson, Marianne, et. al. Guide for Developing Security Plans for Federal Information Systems (NIST Special Publication 800-18 Rev. 1). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Feb. 2006.

<http://csrc.nist.gov/publications/nistpubs/index.html>.

[Taylor 04]

Taylor, Patrick. "A Wake Up Call to All Information Security and Audit Executives: Become Business-Relevant." Information Systems Control Journal 6, 2004.

[Westby 03]

Westby, Jody R., editor. International Guide to Combating Cybercrime. American Bar Association, Privacy & Computer Crime Committee, Section of Science & Technology Law. American Bar Association, 2005. Ordering information available at <http://www.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450030>.

[Westby 04a]

Westby, Jody R., editor. International Guide to Privacy. American Bar Association, Privacy & Computer Crime Committee, Section of Science & Technology Law. American Bar Association, 2004. Ordering information available at <http://www.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450037>.

[Westby 04b]

Westby, Jody R., editor. International Guide to Cyber Security. American Bar Association, Privacy & Computer Crime Committee, Section of Science & Technology Law. American Bar Association, 2004. Ordering information available at <http://www.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450036>.

[Westby 05]

Westby, Jody, editor. "Roadmap to an Enterprise Security Program." American Bar Association, Privacy & Computer Crime Committee, Section of Science & Technology Law. American Bar Association, 2005. Ordering information available at <http://www.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450039>.

[Wilcox 06]

Wilcox, John C. "What's Next for Boards? Ten Landscape-Altering Trends," Directors & Boards, 2006. <http://directorsandboards.com/DBEBRIEFING/November2006/ColumnNovember2006.html>.

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE August 2007	3. REPORT TYPE AND DATES COVERED Final		
4. TITLE AND SUBTITLE Governing for Enterprise Security (GES) Implementation Guide		5. FUNDING NUMBERS FA8721-05-C-0003		
6. AUTHOR(S) Jody R. Westby, Julia H. Allen				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213			8. PERFORMING ORGANIZATION REPORT NUMBER CMU/SEI-2007-TN-020	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) HQ ESC/XPB 5 Eglin Street Hanscom AFB, MA 01731-2116			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12A DISTRIBUTION/AVAILABILITY STATEMENT Unclassified/Unlimited, DTIC, NTIS			12B DISTRIBUTION CODE	
13. ABSTRACT (MAXIMUM 200 WORDS) <p>Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. If an organization's management does not establish and reinforce the business need for effective enterprise security, the organization's desired state of security will not be articulated, achieved, or sustained. To achieve a sustainable capability, organizations must make enterprise security the responsibility of leaders at a governance level, not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance.</p> <p>This implementation guide builds upon prior publications by providing prescriptive guidance for creating and sustaining an enterprise security governance program. It is geared for senior leaders, including those who serve on boards of directors or the equivalent. Throughout the implementation guide, we describe the elements of an enterprise security program (ESP) and suggest how leaders can oversee, direct, and control it, and thereby exercise appropriate governance.</p> <p>Elevating security to a governance-level concern fosters attentive, security-conscious leaders who are better positioned to protect an organization's digital assets, operations, market position, and reputation. This document presents a roadmap and practical guidance that will help business leaders implement an effective security governance program.</p>				
14. SUBJECT TERMS computer security, corporate security, corporate computer security, management, enterprise management, security, security practice			15. NUMBER OF PAGES 116	
16. PRICE CODE				
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	