Governing for Enterprise Security (GES)

Implementation Guide

Article 3: Enterprise Security Governance Activities

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

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

March 2007

Introduction

This article elaborates the description of an enterprise security program (ESP) discussed in Article 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.

The Basis for Governance of Enterprise Security[1]

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.

Proper governance necessarily requires an understanding of the full range of actions and operations involved. Building upon Article 2's explanation of an enterprise security program (ESP), this article provides a more in-depth view of how to govern an ESP and the activities and processes undertaken for that purpose.

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].

[1] See also Article 1: Characteristics of Effective Security Governance and refer to the following references: [Allen 05], [Allen 06a], [Allen 06b], and [Allen 06c].

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 also 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) Convention 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 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].

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 article, 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]

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 1, (ESP Categories, Activities, Responsibilities/Roles, and Artifacts), this article describes which ESP activities require governance action. Governance-based ESP activities are grouped into the Table 1 categories of Governance, Integration and Operations, Implementation and Evaluation, and Capital Planning and Reviews/Audits and are shown in red text in Table 1. Each section also describes the purpose of the artifacts created during each activity.

Table 1 - ESP Categories, Activities, Responsibilities/Roles, and Artifacts*

ENTERPRISE SECURITY PROGRAM*			
CATEGORY	**ACTIVITY SEQUENCE**	**RESP/ROLES**	**ARTIFACTS**
Governance	• **Establish Governance Structure** • **Assign Roles and Responsibilities, indicating Lines of Reporting** • **Develop Top-Level Policies** ↓	**BRC**	• BRC Mission, Goals, Objectives, & Composition • X-Team Mission, Goals & Objectives, & Members • Organizational Chart • Roles & Responsibilities for ESP • Top-level Policies
	• **Inventory Digital Assets** • **Develop & Update System Descriptions** • **Establish & Update Ownership and Custody of Assets** • **Designate Security Responsibilities & Segregation of Duties** ↓	**CSO, BLE, CIO, BM, AO** **BLE, CSO, CIO, BM, AO** **CSO, BLE, CIO, BM, AO** **BRC, CSO**	• Inventory of Assets & Systems[2] • System Descriptions • Ownership & Custody Determined by BLE and Entered on Inventory by CSO • Detailed Security Responsibilities

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

[2] 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**	• **Categorize Assets by Levels of Risk & Magnitude of Harm** • **Determine & Update Necessary Controls** • **Determine & Update Key Performance Indicators & Metrics** ↓	**BRC, CSO, BLE, CPO, GC, BM** **BRC, CSO, CPO, BLE, GC, BM** **BRC, CSO, BLE, CIO, BM, OP**	• Categorization of Assets • Assignment of Controls (by system) • Key Performance Indicators & Metrics
	• **Identify & Update Best Practices & Standards** • **Determine Asset-Specific Security Configuration Settings** ↓	**CSO, CIO, CPO** **CSO**	• Listing of Approved Best Practices & Standards (BP&S) • Report on Implementation of BP&S • Mapping of BP&S to Controls & Metrics • Asset Security Configuration Settings
	• **Develop, Update, & Test Incident Response Plan** • **Develop, Update & Test Crisis Communications Plan** ↓	**BRC, CSO, BLE, CIO, GC, PR** **BRC, CSO** **CSO** **BRC, PR, CSO, CIO, BLE** **BRC, PR, CSO, CIO, BLE** **PR, CSO, CIO**	• 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)**	• **Develop, Update, & Test Business Continuity & Disaster Recovery Plan** • **Develop, Update & Verify 3rd Party & Vendor Requirements** ↓	**BRC, CSO, CIO, BLE, BM, OP** **BRC, CSO, CIO, BLE** **BRC, CSO, CIO, BLE** **BRC, CSO**	• Business Continuity & Disaster Recovery Plan • Business Continuity & Disaster Recovery Plan Test Report • 3rd Party & Vendor Requirements for BC/DR, IR, CC • 3rd Party & Vendor Requirements Verification Report
	• **Develop & Update Change Management Plans** ↓	**CSO, CIO**	• Change Management Plan • Change Management Logs
	• **Develop & Update Enterprise Security Plan** • **BRC Approval of Enterprise Security Plan** ↓	**BRC, CSO** **CSO** **BRC**	• Enterprise Security Plan • ESP Update Report • BRC Approval of Enterprise Security Plan
	• **Develop & Update Security Policies & Procedures** ↓	**CSO, CPO, BLE, HR, GC, PR, BM, OP, AO**	• Security Policies & Procedures
	• **Develop & Update Security System Architecture Plan** ↓	**CSO, CIO**	• Security System Architecture Plan
Implementation **+** **Evaluation**	• **Develop & Update ESP Implementation & Training Plans** • **Implement & Train** ↓	**BRC, CSO, CPO, HR, BLE, PR, CIO, GC, BM, AO, OP** **CSO, BLE, BM, OP** **BRC, CSO, BLE** **CSO, HR**	• Implementation Plan & Results • Training Modules • Training Plan & Schedule • Record of Training

ENTERPRISE SECURITY PROGRAM*			
CATEGORY	**ACTIVITY SEQUENCE**	**RESP/ROLES**	**ARTIFACTS**
Implementation + **Evaluation (cont'd)**	• **Monitor & Enforce Policies & Procedures** ↓	**CSO, GC, HR, CPO, BLE, BM**	• Monitoring & Enforcement Reports
	• **Test & Evaluate System Controls, Policies, & Procedures (can include C&A)** ↓	**CSO, BLE, BM, CA**	• Testing & Evaluation Report of Controls, Metrics, Policies & Procedures
	• **Identify System Weaknesses & Execute Corrective Action Process (POAM)** ↓	**CSO, CA, BLE, BM**	• System POAMs
Capital Planning + **Reviews/ Audits**	• **Issue Authority (or Interim Authority) to Operate** ↓	**BLE**	• Accreditation Decision Letter
	• **Determine Security Business Case, ROI, & Funding** ↓	**BRC, CSO, CFO** **BRC**	• ESP Security Investment Requirements & ROI Analysis • Board Approved Budget
	• **Conduct Formal Review of ESP** • **Conduct Formal Audit of ESP** ↓	**BRC, CSO, X-Team** **BAC, IA, EA, X-Team**	• Annual ESP Report (by CSO) • Annual ESP Audit Report (by IA & EA)
	↻ **Repeat Process at Designated Intervals, Some Activities Ongoing** [3]		

[3] 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.

Governance Category Activities #1 – Structure and Tone

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

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.

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].

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.

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**

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 category (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.[4]

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

[4] 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.

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).

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.

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

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**

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 article, 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.

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.

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]

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

(a) work through potential response scenarios

(b) plan international cooperation with law enforcement

(c) understand the jurisdictional considerations in investigations and prosecutions

(d) establish points of contact and build relationships with necessary public and private sector entities

(e) 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.

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

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)**

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. *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 OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) describe useful risk assessment processes and methods that are instructive and applicable to all organizations.

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.

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.

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
- Security Inputs to Risk Management Plan
- Enterprise Security Strategy

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**

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 article 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 04c]:

- 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.

The Table 2 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 2 – 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**

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 CobIT (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].

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 Security testing tools are valuable aids in evaluating technical controls. (See also a reference in the bibliography for these articles 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].

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

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

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 3rd Party and Vendor Requirements**

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 home page 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.

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.

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].

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

Governance Activities during Integration and Operations #3 – Security Plan

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

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 Article 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.

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

Governance Activities during Implementation and Evaluation – Implement and Train

- **Develop and Update ESP Implementation and Training Plans**

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

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

- **Determine Security Business Case, Return on Investment, and Funding**

Determine Security Business Case, Return on Investment, and Funding

One of the most perplexing areas of cyber security is

(a) understanding how to make a business case that justifies investment and expenditures on security

(b) calculating return on investment

(c) 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:

(a) ESP activities (including security requirements)

(b) POAM corrective actions

(c) training programs

(d) monitoring and enforcement activities

(e) special assistance, such as forensic expertise, outside legal counsel, technical experts

(f) 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

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

- **Conduct Formal Review and Audit of ESP**

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)

Additional Considerations

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's Security Alerts and Current Activity and the SANS Institute's list of Top-20 Internet Security Attack Targets.

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)
- 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)
- The Information Security Forum's The Standard of Good Practice for Information Security
- NIST Special Publications
- The Payment Card Industry Security Standard
- U.S. Department of Defense Security Directives and Instructions

Conclusion

This article serves as a companion to Article 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.

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 article briefly describes the artifacts the result from each activity. Selected artifacts will be described in more detail in future articles.