Governing for Enterprise Security (GES)

Implementation Guide

Article 2: Defining an Effective Enterprise Security Program (ESP)

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

CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office.

Copyright 2007 Carnegie Mellon University

Introduction

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

To be successful, the program requires a security culture and the cooperation of the entire organization. This is achieved by establishing and reinforcing the security "tone" set at the top of the organization, reflected in top-level policies and an effective governance structure. This structure includes a cross-organizational security team, designated key personnel — such as the chief risk officer (CRO), chief security officer (CSO),[1] general counsel (GC), chief information officer (CIO) and others — and the involvement of operational staff. Internal audit has an independent role in auditing the ESP's effectiveness in addressing organizational security risks.

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

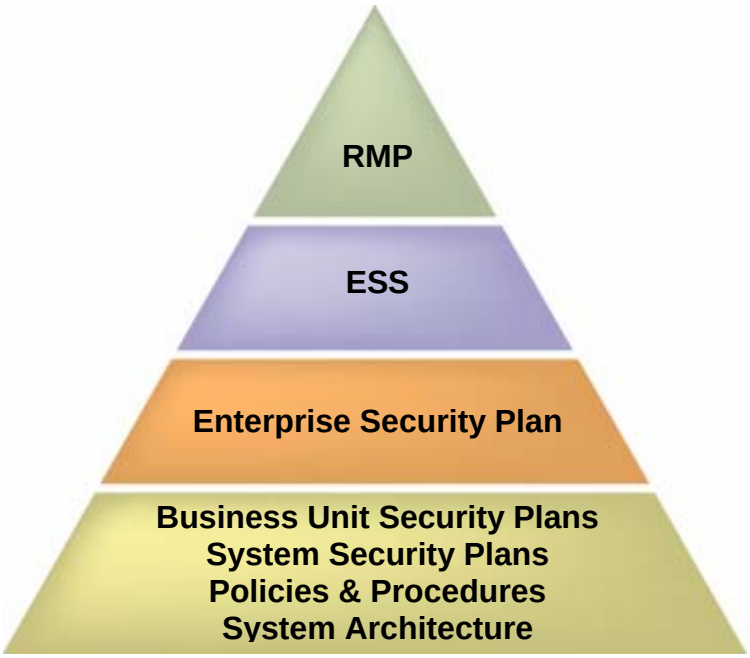
- a long-term enterprise security strategy (ESS)
- an overarching enterprise security plan (which may be supported by underlying business unit security plans and security plans for individual systems)
- security policies, procedures, and other artifacts
- the system architecture and supporting documentation

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

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

Copyright 2007 Carnegie Mellon University

Figure 1 - Enterprise Security Program



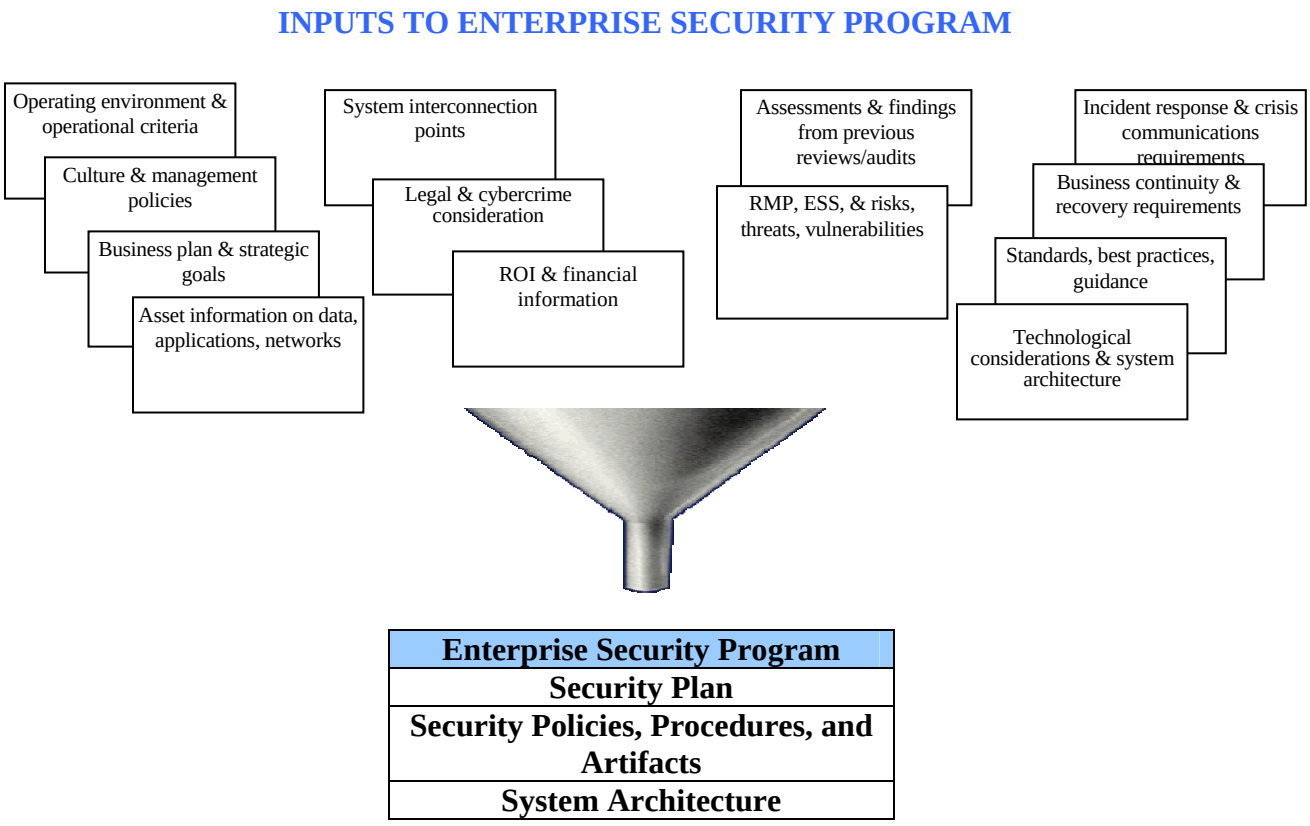
The development and sustainment of an ESP takes into account a wide array of information, including the organization's RMP, ESS, operational criteria[2] and culture, top-level policies, compliance requirements, budget, and system architecture.

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

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

Copyright 2007 Carnegie Mellon University

Figure 2 - Enterprise Security Program Inputs



Copyright 2007 Jody R. Westby

The **enterprise security plan** is the overarching document that serves as the "business plan" for securing an organization's digital assets[3], consisting of [Westby 05]

1. information and data
2. applications[4]
3. networks

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

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

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

[4] This includes operating platforms and supervisory control and data acquisition (SCADA) systems.

Copyright 2007 Carnegie Mellon University

- Top-level (managerial) policies are broad statements that support the risk objectives of the RMP that pertain to security. They govern operations and the use of technology, such as the use of email and wireless devices; remote access to systems; the protection of intellectual property; business continuity; and critical security controls.
- Functional policies cover operational functions, such as the types of information that require privacy and security protections, who can access this information, and where it may be transmitted or stored.
- Computing policies determine the operating environment and cover topics such as network availability and reliability, backup and recovery requirements (including business continuity), and the like.
- Security policies define the security requirements for the organization's operation, such as authentication controls, encryption, basic authorization limits, incident handling and log requirements, and the like.

Policies are comprised of three parts: the policy content, compliance and monitoring information, and enforcement sanctions.[5]

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

ESP requirements are supported and constrained by the **system architecture**.[6] For example, network firewalls support the program's security requirements, but a network's interconnectivity with third party networks may constrain the protection of sensitive information and present special security considerations. In this regard, it is important to remember that the system architecture is determined by business requirements, not vice versa. As a general matter, organizations whose business operations are shaped around the technical environment risk losing productivity and competitiveness.

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

An ESP is comprised of four main categories. Each category represents a sequence of activities (see Table 1) that produce specific artifacts which serve as key inputs to subsequent activities. The four categories of an ESP are [Westby 05]

1. governance
2. integration and operation

---

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

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

Copyright 2007 Carnegie Mellon University

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

The following sections

- discuss the development and sustainment of an ESP
- recommend an organizational structure
- suggest a sequence for the activities performed and the artifacts produced
- assign responsibility for the activities

These sections explain the activities that are specific to governance oversight and action with respect to security, including the basis for governance, the desired approach, and the interaction of personnel. Other key considerations, such as the impact of new technological innovations on the ESP and the use of best practices and standards are highlighted.

Roles

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

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

The involvement of the appropriate personnel and the proper alignment of roles and responsibilities in each of the four ESP categories are critical to the adequacy and effectiveness of the program. There are eight groups of personnel involved in the development and sustainment[7] of an ESP:

1. Board risk committee (BRC)
2. Senior officers of the organization: C-level, such as the chief executive officer (CEO), chief operating officer (COO), and chief administrative officer (CAO)
3. Cross-organizational ESP team (X-Team) comprised of
    - general counsel (GC)
    - chief information officer (CIO)[8]
    - chief security officer (CSO) and/or chief risk officer (CRO)
    - chief privacy officer (CPO)

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

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

Copyright 2007 Carnegie Mellon University

- chief financial officer (CFO)
- business line executives (BLEs)
- communications executives (may also include investor relations) (PR)
- director of human resources (HR)

4. Asset owners (AO)
5. Business managers (BM)
6. Operational personnel, including procurement personnel (OP)
7. Certification agent (CA)
8. Board audit committee (BAC)
9. Internal and external audit personnel (IA, EA)

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

Responsibilities

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

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

Board Risk Committee

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

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

Copyright 2007 Carnegie Mellon University

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

- conducting risk assessments and reviews
- developing, approving, and maintaining the organization's RMP, ESS, and enterprise security plan
- categorizing assets by levels of risk and harm and approving security controls, key performance indicators, and metrics
- steering the development, testing, and maintenance of plans for business continuity and disaster recovery, incident response, crisis communications, and relationships with vendors and other third parties[9]
- allocating sufficient financial resources for the development and sustainment of the program based upon a security business case and return on investment (ROI)
- ensuring the ESP is implemented and personnel are effectively trained according to the implementation and training plan
- conducting periodic (no less than annual) reviews of the ESP
- ensuring material weaknesses in the ESP are rectified and the ESP is up-to-date

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

X-Team

The X-Team is responsible for the coordination of security issues and the implementation of the BRC-approved RMP, ESS, and enterprise security plan, usually under the direction of a senior executive, such as the chief operating officer (COO) in large organizations or the chief executive officer (CEO) in small- to medium-sized organizations. Members of the X-Team have individual and/or shared responsibility for certain ESP activities, which are noted in Table 1. Generally, however, the GC, CSO/CRO, CPO, CIO, and BLEs are the anchor members of the X-Team. They shoulder the greatest responsibility for the ESP, with the CSO taking the lead in its development, implementation, and sustainment.

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

Copyright 2007 Carnegie Mellon University

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

- Asset Management
    - developing and maintaining an inventory of all digital assets (including identifying asset owners and custodians)
    - assigning detailed security responsibilities (including SOD)
- Assessment
    - conducting security threat and risk assessments (the CA may also share the lead role if a system certification is being performed)
- Planning and Strategy
    - providing security input into the development of the RMP
    - developing and maintaining an enterprise security strategy (ESS)[10] that supports the RMP
    - developing, implementing, and maintaining an enterprise security plan
    - developing and maintaining security policies and procedures
    - developing, testing, and maintaining an incident response (IR) plan
    - developing and maintaining security system architecture plan
    - developing and maintaining an ESP training plan and schedule
    - developing security training modules and maintaining training records
    - integrating security requirements into the capital planning and investment process and determining ROI (shared responsibility with CFO)
- Controls and Performance Management
    - determining needed controls, and testing and evaluating their effectiveness
    - ensuring the appropriate security standards and best practices have been implemented and security configuration settings conform to the ESP
    - determining and evaluating security key performance indicators (KPI) and metrics
- Reviews, Certifications, and Audits
    - supervising the certification and accreditation (C&A) of all systems and the development of plans of action and milestones (POAMs)[11]

---

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

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

Copyright 2007 Carnegie Mellon University

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

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

The **CSO and CIO** share responsibility for

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

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

The **GC, CSO/CRO, and CPO** are responsible for ensuring that (a) all security-relevant compliance and contractual requirements and liability risks have been identified, a Table of Authorities[12] is developed, and digital assets are mapped to the Table of Authorities, and (b) security and privacy risks are adequately mitigated in accordance with the organization's RMP, ESS, policies, and code of conduct.

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

The **GC** is responsible for mapping cybercrime and security breach notification laws to data flows.[13]

---

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

[12] A Table of Authorities lists all applicable laws, regulations, directives, contracts, and other legal requirements applicable to the organization's assets and systems.

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

Copyright 2007 Carnegie Mellon University

The GC often takes the lead in investigating breaches or incidents, including gathering and protecting evidence, to ensure that evidentiary considerations are taken into account, communications with law enforcement are coordinated, and liability risks are managed.

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

BLEs are responsible for assigning ownership and custody of their assets, determining operational criteria, and ensuring that their systems meet the requirements of the security plan and are certified and accredited, if required. The BLE issues the letter granting authority to operate (ATO) or interim authority to operate (IATO). Best practices require BLEs to accept or deny the risks associated with their systems through their granting or denying authorizations to operate.[14] This role for the BLE reflects the integration of the ESP throughout the organization and indicates how the system architecture supports business operations. Business executives can no longer insulate themselves from the risks associated with the use of technology to fulfill their operational requirements. The risk that the system brings to the organization, therefore, is borne by the business line. Therein lays the incentive for BLEs to ensure their systems meet compliance requirements, are secure, and have effective controls, policies, and procedures.

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

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

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

Additional Roles

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

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

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

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

Copyright 2007 Carnegie Mellon University

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

- assist with threat and vulnerability assessments
- assist in the identification of appropriate metrics
- participate in the development of policies and procedures
- provide input during the development of BC/DR and IR plans
- assist in planning and developing effective training

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

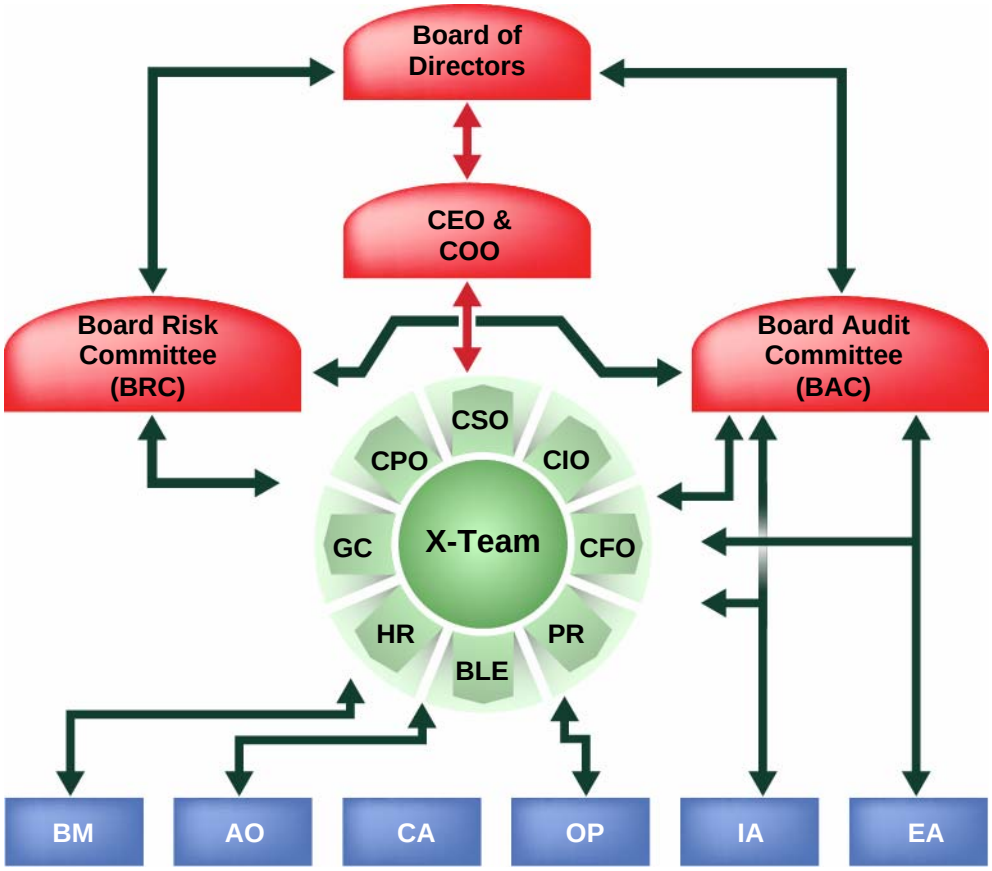
The **CA** is an independent agent who reviews all ESP systems and assesses whether they follow prescribed best practices and standards, have the required artifacts (including ATO or IATO), and meet the requirements of the security plan. Upon completion of the certification process, the CA issues a certification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

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

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

Copyright 2007 Carnegie Mellon University

Figure 3 - Roles Involved in an ESP



Activities and Artifacts

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

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

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

Copyright 2007 Carnegie Mellon University

For each ESP category, Table 1 defines the sequence of activities, the artifacts produced by each activity, and the roles involved. As a result, the figure is useful in describing the scope of the BRC's oversight responsibilities.

In Table 1, all governance activities are listed in red text, and the roles involved in an activity are color-coded, consistent with Figure 3.

Red: **BRC** responsibility

Green: **X-Team** member responsibility

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

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

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

Article 3: Enterprise Security Governance Activities expands and details the governance activities listed in Table 1.

Copyright 2007 Carnegie Mellon University

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[15] • System Descriptions • Ownership & Custody Determined by BLE and Entered on Inventory by CSO • Detailed Security Responsibilities

Copyright 2007 Carnegie Mellon University

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

[15] 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]

Copyright 2007 Carnegie Mellon University

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

Copyright 2007 Carnegie Mellon University

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

Copyright 2007 Carnegie Mellon University

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

[16] 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.

Conclusion

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

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

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

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

Copyright 2007 Carnegie Mellon University