Governing for Enterprise Security Implementation Guide: Sample Artifact

Roles and Responsibilities for an Enterprise Security Program

Scope

This sample artifact describes the leadership roles and responsibilities for the development, implementation, and sustainment of an enterprise security program (ESP), as identified in Article 2: Defining an Effective Enterprise Security Program, Table 1 and Article 3: Enterprise Security Governance Activities. This artifact is not meant to stand alone — rather it should be interpreted in the context of these articles. We hope business leaders will find it useful as an aid in building a governance-based security program.

Introduction

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

X-team members include the

- chief security officer (CSO)[1], chair of the X-team
- chief privacy officer (CPO)
- chief information officer (CIO)
- chief financial officer (CFO)
- general counsel (GC)
- business line executives (BLE)
- vice president of human resources (HR)
- vice president of public relations (PR)

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

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

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

Some responsibilities may be shared, requiring special controls, policies and procedures, and careful coordination. Below, we describe specific roles and responsibilities, followed by the name of the artifact that results from executing a given responsibility.

Detailed security responsibilities for X-team personnel, business managers (BM), operational personnel (OP), and certification agents (CA) are determined by the CSO with oversight by the BRC.

Security responsibilities set by the BRC and CSO help create a culture of security within the organization. They are to be taken seriously. The security responsibilities described here should be included in job descriptions and reviewed as part of performance evaluations.

Roles and Responsibilities

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

Chief Security Officer (CSO)

CSO Responsibilities

The CSO has overall responsibility for the ESP and chairs the X-team. The CSO has direct responsibility for leading and guiding the following activities:

- Develop and maintain an inventory of digital assets, with input and assistance from the BLEs, CIO, BM, and AO. **Artifact: Inventory of Assets and Systems**

- Designate detailed security responsibilities and SOD. **Artifact: Detailed Security Responsibilities**

- Conduct threat, vulnerability, and risk assessments, including system certification and accreditations, with active assistance from the BLE, BM, OP, and CA. **Artifacts: System Risk Assessments**

- Develop and update security inputs to the risk management plan, with assistance from the CPO, CIO, and GC. **Artifact: Security Inputs to Risk Management Plan**

- Develop and update the organization's enterprise security strategy (ESS), with assistance from the CPO. **Artifact: Enterprise Security Strategy**

- Determine and update necessary controls and ensure they are documented in the ESP. The CSO is assisted in this effort by the CPO, BLE, GC, and BM. **Artifact: Assignment of Controls (by system)**

- Determine and update key performance indicators and metrics and ensure they are documented in the ESP. The CSO is assisted in this effort by the BLE, CIO, BM, and OP. **Artifact: Key Performance Indicators and Metrics**

- Identify and maintain a list of security best practices and standards used by the organization, with assistance from the CIO and CPO. Report on the implementation of best practices and standards and map them to controls and metrics. **Artifacts: Listing of Approved Best Practices and Standards; Report on Implementation of Best Practices and Standards; Mapping of Best Practices and Standards to Controls and Metrics**

- Determine asset-specific security configuration settings. **Artifact: Asset Security Configuration Settings**

- Develop, update, and test the organization's incident response plan, with assistance from the BLE, CIO, GC, and PR. Test the incident response plan and report on the results. Produce quarterly reports on incidents. **Artifacts: Incident Response Plan; Incident Response Plan Test Report; Incident Response Reports**

- Develop and update the organization's enterprise security plan. Obtain BRC approval of the ESP. **Artifacts: Enterprise Security Plan; ESP Security Update Report**

- Develop and update security policies and procedures, with assistance from the CPO, BLE, HR, GC, PR, BM, OP, AO. **Artifacts: Security Policies and Procedures**

- Develop and update the security system architecture plan, with assistance from the CIO. **Artifact: Security System Architecture Plan**

- Develop and update the ESP implementation and training plan, with assistance from the CPO, HR, BLE, PR, CIO, GC, BM, AO, and OP. **Artifacts: Implementation Plan and Report of Results**

- Develop training modules, with assistance from BLE, BM, and OP. **Artifacts: Training Modules**

- Develop a training plan and schedule, with assistance from the BLE. **Artifact: Training Plan and Schedule**

- Maintain a record of training, with assistance from HR. **Artifact: Record of Training**

- Test and evaluate system controls, policies, and procedures (this can be part of a certification and accreditation process), with assistance from the BLE, BM, and CA. **Artifact: Testing and Evaluation Report of Controls, Metrics, Policies, and Procedures**

- Conduct a formal review of the ESP, with the assistance of the X-team. **Artifact: Annual ESP Report**

CSO Shared Responsibilities

The CSO shares responsibility with

- the BLE in developing and updating system descriptions. The BLE has responsibility for developing the system descriptions and keeping them current. The CSO has responsibility for ensuring that all required information is collected and entered in the ESP documentation.

- the BLE in establishing and updating ownership and custody of assets. The BLE is responsible for determining ownership and custody of the assets and keeping this information current. The CSO is responsible for gathering this information and recording it in the ESP documentation. **Artifact: Ownership and Custody of Assets**

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

- the GC and CPO in mapping assets to the table of authorities. The CSO and CPO are responsible for ensuring that all assets are included in the mapping exercise.

- the BLE in categorizing assets by levels of risk and magnitude of harm, with assistance from the CPO, GC, and BM. The CSO leads the categorization exercise, and the BLE provides critical input regarding the risk the asset poses to the organization and the magnitude of harm that could result from disruption or loss of the asset. **Artifact: Categorization of Assets**

- the CIO and BLE in developing, updating, and testing a business continuity and disaster recovery (BC/DR) Plan, with assistance from BM and OP. The CSO, CIO, and BLE each bring unique knowledge to the development and maintenance of a BC/DR plan. The CSO has the lead responsibility for gathering the requirements and producing the plan and test report. **Artifacts: BC/DR Plan; BC/DR Test Report**

- the CIO in developing, updating, and verifying third party and vendor security requirements for business continuity and disaster recovery, incident response (IR), and crisis communications (CC), with input from the BLE. The CSO is responsible for gathering the information and preparing associated reports. **Artifacts: Third Party and Vendor Requirements for BC/DR, IR, and CC; Third Party and Vendor Requirements Verification Report**

- the CIO in developing and updating change management plans. The CIO provides input pertaining to operational integrity and availability, and the CSO provides input from the security perspective. **Artifacts: Change Management Plan; Change Management Logs**

- the GC and HR in monitoring and enforcing security policies and procedures, with assistance from the CPO, BLE, and BM. The GC provides input about legal considerations and monitoring restrictions and helps enforce policies and procedures. The HR incorporates monitoring and enforcement policies and procedures into personnel policies and guidelines, and helps enforce policies and procedures. **Artifacts: Monitoring and Enforcement Reports**

- the CA in identifying system weaknesses and executing a corrective action process, with assistance from the BLE and BM. The CSO has the responsibility to ensure the corrective Plan of Action and Milestones is completed and appropriate documentation entered in the ESP.

- the CFO in determining the security business case, including return on investment calculations and funding requirements for the ESP. **Artifact: ESP Security Investment Requirements and ROI Analysis**

CSO Assistance Responsibilities

The CSO assists

- the CPO in mapping and analyzing data flows.

- the GC in mapping cybercrime and security breach notification laws and cross-border cooperation with law enforcement to data flows.

- the CPO in conducting privacy impact assessments and privacy audits.

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

Chief Privacy Officer (CPO)

CPO Responsibilities

The CPO has direct responsibility for

- mapping and analyzing data flows, with the assistance from the CSO, BM, and AO. **Artifact: Mapping and Analysis of Data Flows**

- conducting privacy impact assessments and privacy audits, with assistance from the GC and CSO. **Artifacts: Privacy Impact Assessments; Privacy Audit Reports**

CPO Shared Responsibilities

The CPO shares responsibility with

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

- the CSO and GC in mapping assets to the table of authorities. The CSO and CPO are responsible for ensuring that all assets are included in the mapping exercise.

CPO Assistance Responsibilities

The CPO assists

- the GC in mapping cybercrime and security breach notification laws and cross-border cooperation with law enforcement to data flows.

- the CSO in developing and updating security inputs to the risk management plan.

- the CSO in developing and updating the organization's enterprise security strategy.

- the CSO and BLE in categorizing assets by levels of risk and magnitude of harm.

- the CSO in determining and updating necessary controls.

- the CSO in identifying and maintaining a list of best practices and standards used by the organization.

- the CSO in developing and updating security policies and procedures. The CPO must ensure privacy considerations are taken into account in the policies and procedures.

- the CSO in developing and updating ESP implementation and training plans.

- the CSO, GC, and HR in monitoring and enforcing security policies and procedures.

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

Chief Information Officer (CIO)

CIO Shared Responsibilities

The CIO shares responsibility with

- the CSO and BLE in developing, updating, and testing a business continuity and disaster recovery (BC/DR) plan, with assistance from BM and OP. The CSO, CIO, and BLE each bring specific knowledge to the development and maintenance of a BC/DR plan.

- the CSO in developing, updating, and verifying third party and vendor security requirements for business continuity and disaster recovery, incident response (IR), and crisis communications (CC), with input from the BLE. The CIO provides input regarding network and application requirements and other aspects of IT asset management. The CSO is responsible for gathering the information and preparing associated reports.

- the CSO in developing and updating change management plans. The CIO provides input pertaining to operational integrity and availability, and the CSO provides input from the security perspective.

CIO Assistance Responsibilities

The CIO assists

- the CSO in the development and maintenance of an inventory of digital assets.

- the BLE and CSO in developing and updating system descriptions.

- the CSO and BLE in establishing and updating ownership and custody of assets.

- the CSO in developing and updating security inputs to the risk management plan.

- the CSO in determining and updating key performance indicators and metrics.

- the CSO in identifying and maintaining a list of best practices and standards utilized by the organization.

- the CSO in developing, updating, and testing the organization's incident response plan .

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

- the CSO in developing and updating security system architecture plan.

- the CSO in developing and updating ESP implementation and training plan.

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

Chief Financial Officer (CFO)

CFO Shared Responsibilities

The CFO shares responsibility with

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

CFO Assistance Responsibilities

The CFO assists

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

General Counsel (GC)

GC Responsibilities

The GC has direct responsibility for

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

GC Shared Responsibilities

The GC shares responsibility with

- the CSO and CPO for determining and updating compliance requirements. The GC is responsible for developing and maintaining the table of authorities. The CPO is responsible for ensuring that all applicable privacy laws and regulations have been identified and entered on the table of authorities. The CSO is responsible for ensuring that all applicable security laws and regulations have been identified and entered on the table of authorities. The CSO is responsible for ensuring the table of authorities is entered into the ESP documentation and kept up-to-date. **Artifact: Table of Authorities**

- the CSO and CPO in mapping assets to the table of authorities. The CSO and CPO are responsible for ensuring that all assets are included in the mapping exercise. **Artifact: Mapping of Assets and Authorities**

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

GC Assistance Responsibilities

The GC assists

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

Business Line Executives (BLE)

BLE Responsibilities

The BLE has direct responsibility for

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

BLE Shared Responsibilities

The BLE shares responsibility with

- the CSO in developing and updating system descriptions. The BLE has responsibility for developing the system descriptions and keeping them current. The CSO has responsibility for ensuring that all required information is collected and entered in the ESP documentation. **Artifact: System Descriptions**

- the CSO in establishing and updating ownership and custody of assets. The BLE is responsible for determining ownership and custody of the assets and keeping this information current. The CSO is responsible for gathering this information and recording it in the ESP documentation.

- the CSO in categorizing assets by levels of risk and magnitude of harm, with assistance from the CPO, GC, and BM. The CSO leads the categorization exercise, and the BLE provides critical input regarding the risk the asset poses to the organization and the magnitude of harm that could result from disruption or loss of the asset.

- the CSO and CIO in developing, updating, and testing a business continuity and disaster recovery (BC/DR) plan, with assistance from BM and OP. The CSO, CIO, and BLE each bring specific knowledge to the development and maintenance of a BC/DR plan.

BLE Assistance Responsibilities

The BLE assists

- the CSO in the development and maintenance of an inventory of digital assets.

- the GC, CPO, and CSO in determining and updating compliance requirements on the table of authorities.

- the GC, CSO, and CPO in mapping assets to the table of authorities.

- the GC in mapping cybercrime and security breach notification laws and cross-border cooperation with law enforcement to data flows.

- the CSO in conducting threat, vulnerability, and risk assessments, including system certification and accreditations.

- the CSO in determining and updating necessary controls.

- the CSO in determining key performance indicators and metrics.

- the CSO in developing, updating, and testing the organization’s incident response plan .

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

- the CSO and CIO in developing, updating, and verifying third party and vendor security requirements for business continuity and disaster recovery, incident response (IR), and crisis communications (CC).

- the CSO in developing and updating security policies and procedures.

- the CSO in developing and updating ESP implementation and training plans.

- the CSO in developing training modules to ensure business considerations and requirements are included.

- the CSO in developing the training plan and schedule.

- the CSO, GC, and HR in monitoring and enforcing security policies and procedures.

- the CSO in testing and evaluating system controls, policies and procedures (this can be part of a certification and accreditation process).

- the CA in identifying system weaknesses and executing a corrective action process.

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

Human Resources (HR)

HR Shared Responsibilities

The HR shares responsibility with

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

HR Assistance Responsibilities

The HR assists

- the CSO in developing and updating security policies and procedures. The HR must ensure that compliance with security policies and procedures is embedded in job descriptions and performance evaluations.

- the CSO in developing and updating ESP implementation and training plans.
- the CSO in maintaining a record of training.
- the CSO in conducting a formal review of the ESP.

Public Relations (PR)

PR Responsibilities

The PR has direct responsibility for

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

PR Assistance Responsibilities

The PR assists

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

Business Managers (BM)

BM Assistance Responsibilities

The BM assists

- the CSO in the development and maintenance of an inventory of digital assets.
- the CSO and BLE in developing and updating system descriptions.
- the CSO and BLE in establishing and updating ownership and custody of assets.

- the CPO in mapping and analyzing data flows.
- the CSO in conducting threat, vulnerability, and risk assessments, including system certification and accreditations.
- the BLE in determining operational criteria.
- the CSO and BLE in categorizing assets by levels of risk and magnitude of harm.
- the CSO in determining and updating necessary controls.
- the CSO in determining key performance indicators and metrics.
- the CSO, CIO and BLE in developing, updating, and testing a business continuity and disaster recovery (BC/DR) Plan.
- the CSO in developing and updating security policies and procedures.
- the CSO in developing and updating ESP implementation and training plans.
- the CSO in developing training modules to ensure business considerations and requirements are included.
- the CSO, GC, and HR in monitoring and enforcing security policies and procedures.
- the CSO in testing and evaluating system controls, policies and procedures (this can be part of a certification and accreditation process).
- the CA in identifying system weaknesses and executing a corrective action process.

Operational Personnel (OP)

OP Assistance Responsibilities

The OP assist

- the CSO in conducting threat, vulnerability, and risk assessments, including system certification and accreditations.
- the CSO in determining key performance indicators and metrics.
- the CSO, CIO and BLE in developing, updating, and testing a business continuity and disaster recovery (BC/DR) plan.
- the CSO in developing and updating security policies and procedures.

- the CSO in developing and updating ESP implementation and training plans.
- the CSO in developing training modules to ensure business considerations and requirements are included.

Asset Owners (AO)

AO Assistance Responsibilities

The AO assists

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

Certification Authority (CA)

CA Shared Responsibilities

The CA shares responsibility with

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

CA Assistance Responsibilities

The CA assists

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