risk3sixty

Security Program Organizational Structure

Security Team Operating System

Summary

Leaders ensure the right people are doing the right job to accomplish the mission. In chapter 4, covered how leaders can establish a security organizational structure to support the team's objectives. Use this tool to define roles and responsibilities for your security team. Remember that chapter 4 describes these roles in more detail, so reference the book if you need guidance.

Security Team Operating Model		
Information Risk Council	Security Leadership Team	Initiative Review Board

Office of the CISO	Detect and Respond	Governance Risk and Compliance	Product Security	Third Party Risk	Project Management	Shared Services

Section 1: Security Governance

Note: Depending on the organization size it may be appropriate to have a single governance structure that performs all three duties below.

Information Risk Council (IRC)

An Information Risk Council (IRC) is the link between the security organization and leaders outside the security team. It is a cross-functional committee responsible for overseeing and managing information security risks across the organization. The IRC plays a crucial role in ensuring that information security practices align with business objectives, compliance requirements, and risk tolerance levels.

Role	Name
IRC Chair	

Security Leadership Team (SLT)

The Security Leadership Team (SLT) typically consists of the CISO and their direct reports. They are responsible for setting the overall cybersecurity strategy, vision, and objectives of the organization. The SLT plays a pivotal role in aligning cybersecurity initiatives with business goals and ensuring that the organization's digital assets are adequately protected.

Role	Name
CISO	

Initiative Review Board (IRB)

An Initiative Review Board (IRB) is a decision-making body responsible for assessing proposed cybersecurity initiatives and projects. The IRB ensures that these initiatives align with the organization's strategic goals, resource availability, and risk management strategies.

Role	Name
IRB Chair	

Section 2: Roles and Responsibilities

Note: Depending on the organization size there may be many shared responsibilities or individuals that fulfill multiple roles. It is also common to leverage third parties.

Office of the CISO

This function is responsible for developing and implementing the overall security strategy and policies for the organization. It involves identifying security risks, defining security objectives, and ensuring alignment with business goals.

Role	R	A	C	I
Security Executive				
Report to the Board of Directors				
Information Risk Council Chair				
Security Strategy				
Designing Security Organizational Structure				
Security Program Budget				

Security Tooling and Software Selection				
Media and Public Relations				
Security Communications				
Security Awareness Training				
Managing Key Third Party and Consultant Relationships				

Detection and Response

This function focuses on monitoring, detecting, and responding to security incidents and threats. It involves utilizing various tools and technologies to identify potential security breaches and quickly respond to mitigate their impact.

Role	R	A	C	I
Security Operations Center (SOC)				
Security Monitoring Configuration				
Security Alert Investigation				
Vulnerability Management				
Penetration Testing				
Threat Hunting				
Red Team/Blue Team/Purple Team				
Incident Response (Event Response)				
Incident Response (Planning and Tabletops)				

Governance, Risk, and Compliance (GRC)

This function ensures that the organization complies with applicable laws, regulations, and industry standards. It involves assessing and managing risks, establishing and maintaining compliance frameworks, and monitoring the effectiveness of controls.

Role	R	A	C	I
Risk Assessment				
Risk Register				
Preparation for Information Risk Council Meetings				
Policy				
Compliance (e.g., SOC 2, ISO 27001, PCI DSS)				
Regulatory (e.g., HIPAA, FCRA, GLBA)				
Internal Audits, Control Monitoring, and Certification Readiness				
External Audits (certification and customer audits)				
Customer Trust (Assist during customer due diligence)				

Product Security

This function focuses on securing the organization's products and services throughout their lifecycle, from design and development to deployment and maintenance. It involves integrating security into the product development process and ensuring the security of software and products.

Note: This may be owned by the engineering team for organizations who offer products as part of their services

Role	R	A	C	I
Product Design Security (e.g., how the user interacts with the product)				
Product Security (Application Layer)				
Product Security (Infrastructure Layer)				
SDLC, Security by Design, DevSecOps (Policy)				
Vulnerability Management (Product Level)				
Uptime and Availability				
Product Logging and Security Monitoring				
Incident and Breach Response (Product Level)				
Penetration Testing (Application Layer)				
Penetration Testing (Infrastructure Layer)				

Third Party Risk

This function is responsible for assessing and managing the risks associated with the organization's relationships with third-party vendors, suppliers, and partners. It involves evaluating the security posture of third parties and ensuring their compliance with security requirements.

Role	R	A	C	I
Third Party Risk Management Program Policy				
Performing Vendor Risk Assessments on New Vendors				
Annual Vendor Risk Assessment on Vendor Population				
Supply Chain Risk Assessments				
Review Vendor Contracts for Security Clauses				
Reporting Risks to the Information Risk Council				

Cybersecurity Project Management Office (PMO)

This function provides project management support and oversight for cybersecurity initiatives and programs within the organization. It involves coordinating and prioritizing cybersecurity projects, ensuring their successful execution, and tracking progress.

Role	R	A	C	I
Initiative Program Management (Monitors all major initiatives and reports on status)				
Defines Project Scope				
Develops Project Plan				
Develops Project Budget				
Develops Human Resourcing Plan				
Manages and Reports on Project Plan and Timeline				
Manages and Reports on Project Budget to Actual				
Coordinates Across Teams				
Sends Regular Status Reports				

Shared Responsibilities

This function involves collaboration and coordination with various departments across the organization to address cybersecurity requirements and ensure a holistic approach to security.

Information Technology

Role	R	A	C	I
Corporate Network Security				
Enterprise Application Security				
Email Security				
Asset Management				
Employee Access Provisioning				
Employee Access Removal				
Endpoint Device Management				
Business Continuity (I.T. Systems)				
Disaster Recovery (Backups)				
Patch Management				
Implementation of Hardening Standards on (I.T. Infrastructure)				
Implementation of Hardening Standards on (Perimeter Devices)				
Helpdesk and I.T. Support				

Legal

Role	R	A	C	I
Regulatory Analysis (e.g., FCRA, GLBA)				
Contractual Review				
Incident Response				
Cybersecurity Insurance				
Corporate Communications				
Relationship with Outside Counsel				

Human Resources

Role	R	A	C	I
Employee Onboarding				
Employee Offboarding				
Employee handbook				
Administer Training				

Corporate Risk Management

Role	R	A	C	I
Enterprise Risk Management Standards				
Policy Standards				
Board Reporting and Security Subcommittee				
Corporate Internal Audit Standards				
Facilities				