SCOPE Framework: Roles & Responsibilities

Originating Component	SCOPE Framework Governance Committee
Releasability	Cleared for public distribution. Available in the SCOPE Framework Hub at [https://timtiptonjr.com/scope-hub].

Table of Contents

Purpose: The structure and allocation of cybersecurity roles and responsibilities are influenced by multiple factors, including the size of the organization, industry-specific regulatory requirements, and the overall complexity of the enterprise's information systems. A well-defined cybersecurity governance framework is essential to ensure clear lines of accountability, effective risk management, and the strategic alignment of security initiatives with business objectives.

A robust governance model establishes authority, responsibility, and decision-making processes for cybersecurity functions at all levels of the organization. This includes defining the roles of executive leadership, security operations, risk management personnel, and technical security teams to facilitate coordinated and risk-informed decision-making. The governance framework must integrate cybersecurity into the broader enterprise risk management (ERM) strategy, ensuring that security risks are identified, assessed, and managed in a manner that supports the organization's mission and operational objectives.

Effective cybersecurity governance also requires policy enforcement mechanisms, continuous monitoring, and the ability to adapt to evolving threats. Organizations must delineate responsibilities among leadership, management, and operational staff to prevent ambiguity in security decision-making, improve incident response effectiveness, and enhance compliance with regulatory and contractual obligations. By implementing a structured cybersecurity governance approach, organizations can establish a resilient security posture that proactively addresses risks while enabling business innovation and operational efficiency.

Section 1. Executive Leadership

Executive leadership establishes cybersecurity as a strategic function within the enterprise, ensuring that risk management, compliance, and operational security measures are integrated into overall corporate governance. The following executive roles define the strategic, financial, and operational oversight of an organization's cybersecurity program.

1.1 Chief Executive Officer (CEO)

The Chief Executive Officer (CEO) is the highest-ranking executive in the organization, responsible for setting overall business strategy, financial priorities, and corporate governance. The CEO plays a critical role in defining the organization's risk appetite, ensuring cybersecurity investments align with business objectives, and holding leadership accountable for managing cyber risk.

Key Responsibilities:

i. Establishes cybersecurity as a core business function and ensures it is integrated into enterprise risk management (ERM).
ii. Approves the cybersecurity risk appetite statement, balancing security needs with operational and financial priorities.

iii. Ensures alignment between cybersecurity strategy and overall business objectives, including digital transformation initiatives.
iv. Supports cross-functional collaboration between security, IT, legal, risk management, and finance departments.
v. Provides final authorization for major cybersecurity investments, initiatives, and remediation efforts.
vi. Leads executive-level incident response decision-making during high-impact cybersecurity events.
vii. Engages with board members, regulators, and external stakeholders to discuss cybersecurity governance, compliance, and risk posture.
viii. Ensures that cybersecurity performance metrics are reviewed as part of executive decision-making processes.

1.2 Board of Directors / Cybersecurity Governance Committee

The Board of Directors provides oversight and strategic direction for the organization's cybersecurity governance, ensuring that cyber risks are managed within the organization's overall risk framework. Many organizations establish a Cybersecurity Governance Committee within the board to provide focused oversight on cybersecurity risk management.

Key Responsibilities:

i. Reviews and approves the cybersecurity governance framework, ensuring it aligns with business risk tolerance.
ii. Monitors cybersecurity budget allocations, investments, and return on security expenditures (ROSE).
iii. Holds CISO accountable for implementing an effective cybersecurity strategy.
iv. Reviews and challenges cybersecurity risk assessments and incident response planning.
v. Approves major cybersecurity initiatives, such as Zero Trust adoption, cloud security strategies, or mergers and acquisitions (M&A) risk assessments.
vi. Engages with external regulators, industry groups, and auditors to ensure compliance with applicable laws and regulations.
vii. Oversees cyber risk reporting to ensure that metrics and performance indicators are meaningful and actionable.
viii. Establishes guidelines for cyber risk disclosure and public communications following security incidents or breaches.

1.3 Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) is the executive responsible for the development, implementation, and management of the organization's cybersecurity strategy. The CISO ensures that cybersecurity controls are risk-based, effective, and aligned with both business objectives and regulatory requirements. Unlike the CIO, who focuses on overall IT strategy and infrastructure, the CISO exclusively manages cybersecurity risk and resilience.

Key Responsibilities:

i. Develops and enforces the enterprise-wide cybersecurity strategy, policies, and standards.
ii. Leads cyber risk management efforts, ensuring alignment with regulatory frameworks.
iii. Directs threat intelligence, risk assessment, and incident response programs.
iv. Oversees the Security Operations Center (SOC), vulnerability management, and continuous monitoring initiatives.
v. Collaborates with IT, legal, compliance, and finance teams to integrate cybersecurity into business processes.
vi. Provides cybersecurity risk reporting to executive leadership and the Board of Directors.
vii. Evaluates and prioritizes security investments and technology procurements.
viii. Engages with regulatory bodies, industry groups, and government agencies on cybersecurity matters.
ix. Manages third-party risk assessments, ensuring supply chain security and vendor compliance.
x. Develops security awareness and training programs for employees and executives.

1.4 Chief Information Officer (CIO)

The Chief Information Officer (CIO) is responsible for enterprise IT strategy, digital transformation, and technology infrastructure, ensuring that IT operations support the organization's business goals. While the CIO collaborates with the CISO on cybersecurity initiatives, their focus is on IT performance, innovation, and operational efficiency, rather than security risk management.

Key Responsibilities:

i. Defines the IT strategic roadmap, ensuring alignment with business needs and digital transformation objectives.
ii. Oversees enterprise IT governance, architecture, and infrastructure management.
iii. Ensures technology investments and digital initiatives support business goals.
iv. Works closely with the CISO to ensure secure IT operations and cloud security adoption.
v. Directs IT risk management efforts, ensuring resilience against cyber threats and system failures.
vi. Oversees network, data center, and enterprise application security, in collaboration with the security team.
vii. Ensures IT service continuity and disaster recovery plans are in place and tested.
viii. Balances IT cost management with security requirements to optimize technology spending.

1.5 Chief Risk Officer (CRO)

The Chief Risk Officer (CRO) oversees enterprise-wide risk management, integrating cybersecurity risks into the broader risk management framework. The CRO ensures that cyber risk is assessed, reported, and mitigated in coordination with other business risks such as financial, operational, and reputational risks.

Key Responsibilities:

i. Develops and enforces enterprise risk management (ERM) policies that incorporate cybersecurity risks.
ii. Conducts cyber risk quantification and scenario analysis to measure financial and operational impact.
iii. Ensures cyber risk is factored into business continuity and disaster recovery planning.
iv. Works with the CISO to establish risk tolerance thresholds and prioritize cybersecurity initiatives accordingly.
v. Engages with cyber insurance providers to assess coverage and risk transfer strategies.
vi. Reports to executive leadership and the Board on cyber risk posture and key risk indicators (KRIs).
vii. Coordinates risk assessments for M&A transactions, third-party vendors, and cloud adoption.
viii. Ensures alignment between regulatory compliance, legal obligations, and cybersecurity risk management.

1.6 Chief Financial Officer (CFO)

The Chief Financial Officer (CFO) is responsible for budgeting, financial planning, and investment strategy, including the allocation of cybersecurity resources. The CFO ensures that cybersecurity initiatives align with financial goals while assessing the cost-benefit ratio of security investments.

Key Responsibilities:

i. Allocates budget and financial resources for cybersecurity programs.
ii. Evaluates the return on security investment (ROSI) and cost-benefit analysis of cybersecurity initiatives.
iii. Works with the CISO to assess financial risk exposure related to cybersecurity threats.
iv. Approves cybersecurity procurement and technology investments.
v. Engages in financial risk management and cyber insurance policy selection.
vi. Ensures financial compliance with cyber risk regulations.

1.7 Chief Legal Officer (CLO) / General Counsel

The Chief Legal Officer (CLO) or General Counsel ensures that cybersecurity policies and incident response actions comply with legal and regulatory requirements. The CLO is responsible for cyber liability and legal risk management related to cybersecurity incidents.

Key Responsibilities:

i. Advises executive leadership on cybersecurity legal and regulatory obligations.
ii. Ensures compliance with data privacy laws.
iii. Manages legal aspects of incident response, including breach notifications and regulatory reporting.
iv. Provides guidance on cybersecurity contract clauses for vendors and third parties.
v. Leads legal risk assessments for data security policies and cyber risk disclosures.
vi. Supports litigation or regulatory investigations related to data breaches and cyber incidents.

1.8 Chief Audit Executive (CAE)

The Chief Audit Executive (CAE) is responsible for overseeing the internal audit function, 1ensuring that cybersecurity risks, controls, and compliance measures are effectively assessed and independently validated. The CAE provides an unbiased evaluation of the organization's security posture, governance frameworks, and risk management strategies, reporting directly to executive leadership and the Board of Directors. Unlike the CISO, who is responsible for implementing security controls, the CAE's role is to assess, audit, and verify the effectiveness of cybersecurity programs through an independent lens.

Key Responsibilities:

i. Develops and executes an independent audit strategy to assess cybersecurity risk management and compliance.
ii. Conducts internal audits of security controls, policies, and procedures to ensure alignment with regulatory frameworks.
iii. Reports findings and audit recommendations to the Board, Audit Committee, and executive leadership, ensuring corrective actions are implemented.
iv. Evaluates the effectiveness of security risk management frameworks and ensures proper governance structures are in place.
v. Ensures continuous audit and assurance mechanisms are implemented to track security performance and incident response capabilities.
vi. Oversees cybersecurity-related fraud risk assessments and investigations in coordination with legal and compliance teams.
vii. Assesses the security implications of third-party relationships, including vendor risk management and supply chain security audits.
viii. Engages in regulatory and compliance reporting, ensuring that cybersecurity audit processes support industry and legal requirements.

Section 2. Cybersecurity Strategy and Risk Management

Effective cybersecurity governance requires the establishment of distinct roles to oversee strategic security initiatives, risk management, compliance, and regulatory adherence. The following roles are responsible for ensuring that cybersecurity policies, frameworks, and risk mitigation strategies align with business objectives while maintaining resilience against emerging threats.

2.1 Vice President (VP) or Director of Cybersecurity

The Vice President or Director of Cybersecurity provides leadership in the execution of the enterprise-wide cybersecurity strategy, ensuring that security policies, technologies, and initiatives align with business objectives, risk tolerance, and regulatory requirements. This role bridges the gap between executive leadership and technical security teams by translating high-level strategic goals into actionable security programs.

Key Responsibilities:

i. Develops and executes the organization's cybersecurity strategy, ensuring alignment with enterprise risk management and business continuity objectives.
ii. Directs the implementation of cybersecurity programs, ensuring appropriate resource allocation, staffing, and technology investments.
iii. Establishes, maintains, and enforces cybersecurity policies, standards, and procedures in compliance with applicable regulations and industry best practices.
iv. Oversees the continuous improvement of the organization's security posture by driving advancements in security processes, risk management methodologies, and operational effectiveness.
v. Communicates cybersecurity risks, objectives, and performance metrics to senior executives and board members, advocating for necessary security investments.
vi. Manages cybersecurity budgets, ensures cost-effective investments, and prioritizes security initiatives based on risk assessments and business impact analysis.
vii. Serves as the primary liaison between security teams, IT, legal, compliance, and business units to facilitate the integration of security considerations into organizational workflows.
viii. Provides strategic oversight for incident response activities, ensuring that response plans align with regulatory requirements and business continuity goals.

2.2 Cybersecurity Risk Manager

The Cybersecurity Risk Manager is responsible for identifying, assessing, and mitigating cybersecurity risks across the enterprise. This role ensures that risk management processes are effectively integrated into the organization's security strategy, providing a structured approach to evaluating potential threats, vulnerabilities, and business impacts.

Key Responsibilities:

i. Conducts comprehensive risk assessments to identify security threats, vulnerabilities, and the potential business impact of cyber incidents.
ii. Develops and implements risk treatment plans, balancing security needs with business requirements while ensuring that residual risks remain within acceptable thresholds.
iii. Utilizes risk modeling techniques, quantitative risk analysis, and cybersecurity metrics to communicate risk exposure to executive leadership and key stakeholders.
iv. Evaluates and monitors the cybersecurity risks posed by third-party vendors, contractors, and supply chain partners, ensuring compliance with contractual security obligations.
v. Ensures cybersecurity risk management processes align with regulatory frameworks.
vi. Continuously monitors emerging cyber threats, geopolitical risks, and industry-specific attack trends, updating risk models accordingly.
vii. Supports the incident response function by assessing the potential impact of security incidents and advising on risk-informed response strategies.
viii. Develops and delivers risk awareness programs for employees, ensuring that all personnel understand their role in managing cybersecurity risks.

2.3 Security Compliance & Governance Manager

The Security Compliance & Governance Manager ensures the organization's adherence to cybersecurity policies, regulatory requirements, and industry standards. This role is responsible for developing governance frameworks that support a structured, repeatable approach to compliance while reducing regulatory risk.

Key Responsibilities:

i. Establishes and maintains cybersecurity policies, standards, and guidelines, ensuring alignment with business and regulatory requirements.
ii. Monitors and enforces compliance with applicable laws, regulations, and frameworks.
iii. Manages internal and external cybersecurity audits, ensuring timely completion and remediation of audit findings.
iv. Assesses vendor and partner compliance with cybersecurity requirements, ensuring contractual obligations include adequate security controls.
v. Develops training programs to enhance employee understanding of compliance requirements, security policies, and industry best practices.
vi. Regularly reviews and updates cybersecurity governance structures to reflect evolving threats, business changes, and regulatory updates.
vii. Provides executive leadership with compliance status reports, highlighting key risks, security gaps, and remediation efforts.
viii. Works closely with the legal team to interpret regulatory changes and implement necessary security control adjustments.

Section 3. Security Architecture & Engineering

A well-defined security architecture and engineering function is critical to ensuring the confidentiality, integrity, and availability of enterprise systems, applications, and data. These roles are responsible for designing, implementing, and maintaining security controls that align with organizational objectives, regulatory requirements, and industry best practices. Security architects establish the high-level security framework, while security engineers and DevSecOps practitioners ensure its practical implementation through technical solutions and automation.

3.1 Security Architect

The Security Architect is responsible for designing and maintaining the enterprise-wide security architecture to protect organizational assets from cyber threats. This role ensures that security principles are embedded into IT infrastructure, cloud environments, applications, and business processes. Security Architects develop security models, reference architectures, and roadmaps that align with business objectives while ensuring compliance with industry standards and regulatory frameworks.

Key Responsibilities:

i. Develops and maintains security architecture frameworks, ensuring alignment with business, IT, and cybersecurity strategies.
ii. Defines architectures for Zero Trust Network Access (ZTNA), micro-segmentation, and least privilege access to enhance security resilience.
iii. Designs multi-cloud security architectures, integrating cloud-native security controls, encryption, and identity management solutions.
iv. Defines technical security control baselines, ensuring alignment with relevant frameworks.
v. Conducts security architecture reviews to identify and mitigate risks associated with IT systems, applications, and third-party integrations.
vi. Establishes cryptographic requirements for data-at-rest, data-in-transit, and key management solutions.
vii. Assesses and recommends security tools, such as firewalls, SIEMs, EDR solutions, API security platforms, and identity federation systems.
viii. Designs authentication and authorization architectures, ensuring proper implementation of SSO, MFA, and Privileged Access Management (PAM).
ix. Works with development teams to ensure secure coding practices, threat modeling, and vulnerability management are integrated into the Software Development Lifecycle (SDLC).
x. Provides guidance on security incidents, forensic investigations, and adversary simulations (red/purple team exercises).
xi. Ensures architectural designs meet regulatory requirements and withstand security audits.

3.2 Security Engineer

The Security Engineer is responsible for implementing and maintaining security technologies that enforce the organization's security architecture and policies. This role ensures that security controls are deployed, configured, and continuously optimized to protect enterprise IT environments, cloud services, and endpoints. Security Engineers also assist in vulnerability management, security automation, and incident response.

Key Responsibilities:

i. Implements and configures security solutions, such as firewalls, IDS/IPS, endpoint security (EDR/XDR), SIEM, and identity management systems.
ii. Conducts system and network hardening following CIS Benchmarks, DISA STIGs, and other best practices to reduce attack surfaces.
iii. Assesses OS, application, and cloud vulnerabilities, applies patches, and verifies remediation through validation testing.
iv. Enforces security policies in cloud infrastructure, integrating native cloud security services.
v. Implements role-based access control (RBAC), identity federation, and PAM solutions to restrict unauthorized access.
vi. Configures log collection, normalization, and analytics for SIEM, UEBA, and SOAR platforms to detect and respond to threats.

vii. Supports security operations teams by investigating alerts, containing security incidents, and remediating system compromises.
viii. Develops and maintains security scripts and Infrastructure as Code (IaC) solutions using tools.
ix. Assists in internal and external penetration testing, red team exercises, and remediates findings from ethical hacking assessments.
x. Ensures data encryption, tokenization, and digital certificate management across IT systems and cloud platforms.
xi. Enforces compliance with security standards and audits security configurations against regulatory requirements.

3.3 DevSecOps Engineer

The DevSecOps Engineer is responsible for integrating security into the software development lifecycle (SDLC) and ensuring that security controls are embedded in DevOps pipelines. This role automates security testing, enforces secure coding practices, and collaborates with developers to address security vulnerabilities early in the development process.

Key Responsibilities:

i. Embeds security into CI/CD pipelines, ensuring that code undergoes static analysis (SAST), dynamic analysis (DAST), and dependency scanning (SCA) before deployment.
ii. Develops automated security enforcement mechanisms.
iii. Implements security controls for Docker, Kubernetes (K8s), and serverless architectures, applying Kubernetes RBAC, Pod Security Policies, and Runtime Protection.
iv. Enforces OWASP Top 10 mitigations, code signing, and API security best practices in cloud-native and microservices environments.
v. Ensures proper handling of API keys, tokens, and passwords using secret management tools.
vi. Automates and enforces security testing for web applications, APIs, and mobile applications, ensuring secure application deployment.
vii. Develops real-time alerting mechanisms for DevSecOps pipelines to detect anomalous behaviors, unauthorized changes, and potential code tampering.
viii. Ensures that DevOps workflows align with regulatory and compliance requirements.
ix. Works with security architects and offensive security teams to identify potential attack vectors, misconfigurations, and exploitation paths within DevOps pipelines.

Section 4. Security Operations & Incident Response

Security Operations and Incident Response (IR) functions play a critical role in detecting, analyzing, responding to, and mitigating cybersecurity threats that may impact the confidentiality, integrity, and availability of enterprise systems and data. These roles are structured to provide real-time threat detection, active defense, and incident containment through coordinated processes, leveraging security technologies, intelligence, and forensic analysis. Security Operations Center

(SOC) personnel are responsible for continuous monitoring, alert triage, and escalation, while Incident Response teams investigate, contain, and remediate security incidents. These teams work in close collaboration to minimize the impact of security threats and ensure business continuity.

4.1 Security Operations Center (SOC) Manager

The SOC Manager is responsible for leading and overseeing the daily operations of the Security Operations Center. This role ensures that the organization's security monitoring, detection, and response capabilities are effective, continuously improving, and aligned with industry best practices. The SOC Manager serves as the primary decision-maker for escalated security incidents, facilitates coordination across IT and business units, and ensures compliance with regulatory security requirements.

Key Responsibilities:

i. Develops and maintains the SOC's operational strategy, ensuring alignment with enterprise risk management and cybersecurity objectives.
ii. Ensures continuous monitoring of enterprise environments, including on-premises, cloud, hybrid, and remote assets.
iii. Establishes escalation protocols for alerts, anomalies, and security events, ensuring efficient triage and prioritization.
iv. Directs the use of threat intelligence feeds, adversary TTPs (Tactics, Techniques, and Procedures), and emerging cyber threat insights to enhance detection capabilities.
v. Oversees the tuning and calibration of SIEM, SOAR, XDR, and UEBA solutions, ensuring accurate and timely detections.
vi. Works closely with Incident Response and Digital Forensics teams to facilitate containment and remediation of security breaches.
vii. Ensures adherence to regulatory mandates and prepares reports for auditors and executive leadership.
viii. Establishes SOC effectiveness metrics (MTTD, MTTR, false positive rate, dwell time, etc.) and continuously enhances detection and response capabilities.
ix. Provides incident summaries, risk assessments, and SOC performance reports to executive leadership and the board.

4.2 Incident Response (IR) Lead

The Incident Response Lead is responsible for managing the full lifecycle of security incidents, from detection and analysis to containment, eradication, and recovery. This role leads forensic investigations, implements response strategies, and ensures that incident handling processes align with regulatory and compliance requirements. The IR Lead also conducts post-incident reviews and tabletop exercises to improve the organization's cyber resilience.

Key Responsibilities:

i. Leads the detection, analysis, containment, eradication, and recovery phases of cybersecurity incidents.

ii. Conducts forensic investigations on compromised systems, logs, network traffic, and malware samples to determine attack vectors.
iii. Works closely with SOC analysts, security engineers, legal teams, and executive leadership during high-severity incidents.
iv. Maintains and updates IR playbooks for various attack scenarios (ransomware, insider threats, APT activity, etc.), ensuring rapid and consistent response.
v. Implements containment strategies, including endpoint isolation, network segmentation, and privileged access lockdown.
vi. Conducts after-action reviews (AARs), ensuring that findings are documented and corrective actions are implemented.
vii. Develops and facilitates cybersecurity incident response exercises, improving readiness for various attack scenarios.
viii. Works with legal teams to ensure regulatory requirements are met during breach response and proper reporting to law enforcement or regulators.

4.3 Threat Intelligence Analyst

The Threat Intelligence Analyst is responsible for collecting, analyzing, and disseminating actionable threat intelligence to improve security detection and response. This role tracks threat actors, attack methodologies, and geopolitical cyber threats, integrating intelligence into security operations and strategic risk management.

Key Responsibilities:

i. Gathers intelligence from open-source (OSINT), commercial feeds, dark web monitoring, and government sources.
ii. Analyzes threat actor behaviors, Tactics, Techniques, and Procedures (TTPs), and indicators of compromise (IOCs) to inform security operations.
iii. Enriches SIEM, XDR, IDS/IPS, and endpoint security solutions with contextual intelligence to improve detections.
iv. Works with SOC analysts and IR teams to proactively hunt for indicators of cyber threats in network and endpoint environments.
v. Engages with Information Sharing and Analysis Centers (ISACs), private intelligence sharing groups, and government cybersecurity organizations.
vi. Provides intelligence briefings to executive leadership and risk management teams, highlighting cybersecurity trends, geopolitical risks, and sector-specific threat developments.
vii. Produces detailed threat reports on ransomware groups, APTs, and novel attack techniques, ensuring that security teams are prepared for evolving threats.

4.4 Security Analyst (SOC Analyst - Tier 1 & Tier 2)

Security Analysts are responsible for real-time security monitoring, event triage, and initial investigation of security alerts. They play a key role in identifying potential threats, escalating incidents, and refining security detections.

Key Responsibilities:

i. Analyzes security logs, network traffic, and endpoint alerts for anomalous behavior, unauthorized access, and active cyber threats.
ii. Conducts log correlation, intrusion detection analysis, and malware sandboxing to assess security incidents.
iii. Uses behavioral analysis, MITRE ATT&CK tactics, and threat intelligence to proactively identify undetected threats.
iv. Works with security engineers to improve detection rules, correlation logic, and response automation.
v. Engages IR teams, network security engineers, and business stakeholders for further investigation and mitigation of security incidents.
vi. Follows established SOC runbooks for containment actions, investigation procedures, and forensic collection protocols.