Roles and Responsibilities in Security Governance

Executive Summary

This document provides a comprehensive overview of the essential roles and responsibilities within an organization's security governance framework. Effective security governance is paramount for aligning information security activities with overarching business objectives and regulatory mandates. It necessitates a clear delineation of duties across all organizational tiers, from the board of directors to individual employees, thereby fostering accountability, mitigating security gaps, and facilitating agile decision-making. This material delves into various governance structures, key security roles, committee functionalities, stakeholder engagement methodologies, and best practices for the ongoing documentation and maintenance of robust governance frameworks. A thorough understanding of these roles is indispensable for establishing adaptive and effective security governance capable of responding to evolving business demands and emerging threats, all while maintaining strict adherence to organizational goals and regulatory compliance.

1. Introduction

Information security governance serves as a cornerstone of effective organizational governance, ensuring that all security-related endeavors are meticulously aligned with strategic business goals and regulatory imperatives. The establishment of clear roles and responsibilities throughout an organization is fundamental to achieving robust security. This clarity not only enhances accountability but also proactively addresses potential vulnerabilities and streamlines critical security decisions. This document systematically explores the diverse roles and responsibilities inherent in security governance structures, illustrating how various stakeholders collectively contribute to an organization's overall security posture. We will examine prevalent governance frameworks, define pivotal security roles, detail committee structures, outline effective stakeholder engagement strategies, and present best practices for the comprehensive documentation and sustained maintenance of governance structures. Cultivating a profound understanding of these roles and responsibilities is crucial for developing security governance mechanisms that are both resilient and adaptable, capable of navigating dynamic business landscapes and emerging security threats while consistently upholding organizational objectives and regulatory compliance.

2. Governance Structures and Frameworks

2.1. Hierarchical vs. Matrix Governance Models

Security governance structures typically adopt either a hierarchical or a matrix model, each presenting distinct advantages and challenges. Organizations often implement a hybrid approach, integrating elements from both models to suit their specific operational needs, size, industry, and regulatory environment.

Hierarchical Governance Model:

- Clear lines of authority and reporting.
- Centralized decision-making processes.
- Simplified accountability structures.
- Potential challenges in achieving cross-functional coordination.
- May exhibit reduced adaptability in complex, rapidly evolving environments.

Matrix Governance Model:

- Features dual reporting relationships (functional and administrative).
- Fosters enhanced cross-functional collaboration.
- Offers flexible resource allocation.
- May encounter challenges related to conflicting priorities.
- Requires robust communication protocols to prevent confusion.

2.2. Common Security Governance Frameworks

Several established frameworks provide invaluable guidance for the implementation of effective security governance:

- **ISO/IEC 27014:2020 - Governance of Information Security:** This framework provides foundational principles for governing information security, defining processes for the evaluation, direction, monitoring, and communication of security activities. It strongly emphasizes the alignment of security with business objectives and stakeholder needs.

- **COBIT (Control Objectives for Information and Related Technologies):** A comprehensive IT governance framework that integrates security governance. COBIT effectively bridges the gap between technical issues, business risks, and control requirements, utilizing the RACI model (Responsible, Accountable, Consulted, Informed) to define roles and responsibilities.

- **NIST Cybersecurity Framework (CSF):** This framework offers a policy-based approach to managing cybersecurity risk, incorporating governance aspects within its

"Identify" function. It underscores the importance of understanding business context, resources, and associated risks.

- **ITIL (Information Technology Infrastructure Library):** A service management framework that includes security governance components. ITIL defines security management processes and roles, emphasizing continuous improvement and service alignment.

- **Three Lines Model (formerly Three Lines of Defense):** This model delineates responsibilities into three lines: the first line (operational management) owns and manages risks; the second line (risk management and compliance functions) oversees risks; and the third line (internal audit) provides independent assurance. Board and executive management provide overarching oversight.

2.3. Regulatory Influences on Governance Structures

Regulatory requirements significantly shape security governance structures, particularly within highly regulated industries:

- **Financial Services:** Regulations such as SOX (Sarbanes-Oxley Act), GLBA (Gramm-Leach-Bliley Act), and PCI DSS (Payment Card Industry Data Security Standard) mandate specific governance controls and roles.
- **Healthcare:** HIPAA (Health Insurance Portability and Accountability Act) necessitates designated security officers and formal governance processes.

- **Critical Infrastructure:** Sector-specific regulations frequently mandate specialized security governance structures.
- **Global Operations:** Organizations operating globally must adapt their governance frameworks to comply with regional regulations, such as GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act).

Effective governance structures must be meticulously designed to address these regulatory requirements while retaining sufficient flexibility to adapt to evolving business needs and emerging threats.

3. Key Security Governance Roles

3.1. Overview of Security Governance Roles

Security governance encompasses a multitude of roles across various organizational levels, each endowed with specific responsibilities and authority. These roles collectively form a comprehensive governance structure that ensures security considerations are integrated from strategic planning through to operational implementation. The primary categories of security governance roles include:

- **Board and Executive Leadership:** Comprising the Board of Directors, Chief Executive Officer (CEO), and the Executive Committee.
- **Security Leadership:** Including the Chief Information Security Officer (CISO), Chief Security Officer (CSO), Chief Information Officer (CIO), Chief Risk Officer (CRO), and Chief Privacy Officer (CPO).
- **Security Management:** Encompassing Security Directors, Security Managers, and Security Architects.
- **Operational Security:** Consisting of Security Analysts, Security Engineers, and Security Operations Center (SOC) Staff.
- **Business Unit Representatives:** Such as Business Information Security Officers (BISOs) and Security Champions, as well as Department Managers.
- **Oversight and Assurance:** Including Internal Audit, Compliance Officers, and Risk Management Staff.
- **External Parties:** Such as Regulators, External Auditors, and Security Service Providers.

Each of these roles contributes uniquely to the overall security governance framework, with responsibilities spanning policy development, risk management, control implementation, monitoring, and reporting.

3.2. Role Mapping to Governance Activities

Effective security governance necessitates a clear mapping of specific roles to key governance activities to ensure clear ownership and accountability, thereby preventing gaps or overlaps in responsibility. The following table illustrates this mapping:

Governance Activity	**Primary Roles**	**Supporting Roles**
Strategy Development	Board, CEO, CISO	CIO, CRO, Business Executives
Policy Approval	Board, Executive Committee	CISO, Legal, Compliance
Risk Oversight	Board Risk Committee, CRO	CISO, Internal Audit
Program Direction	CISO, CSO	Security Directors, CIO

Governance Activity	Primary Roles	Supporting Roles
Resource Allocation	CEO, CFO, CIO	CISO, Security Directors
Performance Monitoring	Board, Executive Committee	CISO, Internal Audit
Compliance Oversight	Compliance Committee, CISO, CPO	Legal, Internal Audit
Incident Response	Crisis Management Governance Committee	CISO, Legal, Communications

4. Board and Executive Responsibilities

4.1. Board of Directors' Security Governance Role

The Board of Directors bears the ultimate responsibility for security governance, providing essential oversight and strategic direction. Key responsibilities include:

- **Strategic Oversight:** Ensuring that the security strategy aligns seamlessly with business objectives, approving the overarching security vision, and validating that security investments effectively support business goals.
- **Risk Governance:** Defining the organization's risk appetite and tolerance levels, reviewing and approving the enterprise security risk management approach, and ensuring that major security risks are identified, assessed, and managed appropriately.
- **Resource Allocation:** Approving security budgets and significant investments, ensuring adequate resources are allocated for security programs, and balancing security investments against other critical business priorities.
- **Compliance Oversight:** Ensuring adherence to relevant laws and regulations, reviewing significant compliance issues and their remediation plans, and approving frameworks for managing compliance obligations.
- **Performance Monitoring:** Reviewing the effectiveness of the security program, monitoring key security metrics and indicators, and ensuring the continuous improvement of security capabilities.

Many boards, particularly in larger organizations or regulated industries, establish dedicated risk or technology committees to focus specifically on security governance matters.

4.2. CEO and Executive Committee Responsibilities

The CEO and the Executive Committee are instrumental in translating board-level directives into actionable organizational initiatives. Their responsibilities include:

- **Security Leadership:** Establishing a pervasive security-conscious culture, demonstrating unwavering commitment to security through both words and actions, and ensuring that security considerations are integral to all strategic business decisions.
- **Organizational Structure:** Defining the security governance structure, establishing clear reporting lines for security functions, and ensuring that security leaders are vested with appropriate authority.

- **Resource Management:** Allocating resources based on identified risk priorities, balancing security requirements with broader business objectives, and ensuring that security investments deliver demonstrable value.
- **Performance Accountability:** Holding business units accountable for their security performance, regularly reviewing security metrics and program effectiveness, and taking decisive corrective action when security goals are not met.
- **Crisis Leadership:** Leading the organization through significant security incidents, making critical decisions during security crises, and ensuring appropriate communication with stakeholders during such events.

The Executive Committee typically comprises the CEO, CFO, COO, CIO, and other C-level executives who collectively ensure that security is seamlessly integrated into daily business operations and decision-making processes.

4.3. Board Reporting and Communication

Effective communication between security leadership and the board is paramount for sound governance. This includes:

- **Reporting Framework:** Implementing regular security briefings (typically quarterly), conducting annual comprehensive security program reviews, and ensuring immediate notification of significant security events.
- **Key Reporting Areas:** Providing updates on the security risk posture and any significant changes, major security initiatives and their progress, compliance status and regulatory developments, summaries of security incidents and lessons learned, and emerging threats with strategic responses.
- **Effective Communication Approaches:** Focusing on business impact rather than technical details, utilizing clear metrics and trend analysis, providing essential context for security issues and recommendations, including benchmarking against industry peers, and presenting options with associated risks and benefits.
- **Board Security Education:** Conducting regular board education sessions on pertinent security topics, providing updates on the evolving threat landscape, facilitating scenario-based discussions of security risks, and incorporating external expert perspectives on security trends.

Boards increasingly expect security leaders to articulate security matters in business terms, emphasizing risk, value, and strategic alignment, rather than focusing solely on technical details or compliance checklists.

5. Security Leadership Roles

5.1. Chief Information Security Officer (CISO)

The CISO is the senior executive responsible for establishing and maintaining the enterprise security vision, strategy, and program. Key responsibilities include:

- **Strategic Leadership:** Developing and implementing the overarching security strategy, aligning security initiatives with business objectives, and advising executive leadership on all security matters.
- **Program Management:** Establishing the security management framework, overseeing security policies, standards, and procedures, and managing the security organization and its resources.
- **Risk Management:** Identifying and assessing security risks, developing effective risk treatment strategies, and reporting on the organization's risk posture to executive leadership and the board.

- **Compliance Oversight:** Ensuring compliance with all relevant security requirements, overseeing the security aspects of regulatory compliance, and managing security audit and assessment activities.
- **Security Operations:** Overseeing security monitoring and incident response, ensuring the effective implementation of security controls, and managing security technology and services.

5.2. CISO Reporting Structures

The CISO's reporting relationship significantly influences their effectiveness and organizational influence. Common reporting structures include:

- **Reporting to CIO:** This is a traditional model, offering close alignment with IT strategy and operations but potentially leading to conflicts between IT delivery and security objectives.
- **Reporting to CEO:** An emerging model in security-mature organizations, providing direct board access and elevated security visibility, though it may lack IT operational context.
- **Reporting to CRO:** Common in financial services and regulated industries, offering strong alignment with enterprise risk management but potentially reducing focus on technical security aspects.
- **Reporting to COO:** A growing model in operationally-focused organizations, integrating security with business operations but potentially emphasizing operational over strategic concerns.
- **Reporting to Legal/Compliance:** Seen in highly regulated environments, providing strong compliance alignment but potentially overemphasizing compliance at the expense of comprehensive risk management.

The optimal reporting structure is contingent upon the organization's size, industry, and regulatory landscape.

6. Operational Security Roles

6.1. Security Analysts

Security Analysts are responsible for the day-to-day monitoring and analysis of security events. Their key responsibilities include:

- **Threat Monitoring:** Continuously monitoring security systems, logs, and alerts for suspicious activities or indicators of compromise.
- **Incident Detection:** Identifying and escalating potential security incidents based on analysis of security data.
- **Vulnerability Management:** Assisting in the identification, assessment, and remediation of vulnerabilities within systems and applications.
- **Security Tool Management:** Configuring, maintaining, and optimizing security tools such as SIEM (Security Information and Event Management) systems, intrusion detection/prevention systems (IDPS), and antivirus solutions.
- **Reporting:** Generating regular reports on security posture, incidents, and compliance.

6.2. Security Engineers

Security Engineers design, build, and implement security systems and controls. Their responsibilities include:

- **Security Architecture Design:** Designing secure network architectures, systems, and applications.
- **Control Implementation:** Implementing and configuring security controls, including firewalls, VPNs, encryption, and access control systems.

- **Security Testing:** Conducting security testing, such as penetration testing and vulnerability assessments, to identify weaknesses.
- **Automation:** Developing and implementing security automation scripts and tools to enhance efficiency and effectiveness.
- **Documentation:** Creating and maintaining detailed documentation of security configurations, procedures, and architectures.

6.3. Security Operations Center (SOC) Staff

SOC Staff are at the forefront of an organization's defense, providing continuous monitoring and rapid response to security incidents. Their responsibilities include:

- **24/7 Monitoring:** Operating and monitoring security systems around the clock to detect and respond to threats.
- **Incident Response:** Executing incident response procedures, including containment, eradication, recovery, and post-incident analysis.
- **Threat Intelligence:** Utilizing threat intelligence to proactively identify and mitigate emerging threats.
- **Forensics:** Conducting digital forensics investigations to determine the scope and impact of security incidents.
- **Collaboration:** Collaborating with other IT and business teams during incident response and security initiatives.

7. Business Unit Responsibilities

7.1. Business Information Security Officers (BISOs)

BISOs act as a crucial liaison between the central security function and specific business units. Their responsibilities include:

- **Security Advocacy:** Promoting security awareness and best practices within their respective business units.
- **Risk Assessment:** Conducting business-specific risk assessments and ensuring that security risks are understood and managed within the business context.
- **Policy Implementation:** Ensuring that enterprise security policies and standards are effectively implemented and adhered to within the business unit.
- **Security Requirements:** Translating business requirements into security requirements and vice versa.
- **Reporting:** Reporting on the security posture and compliance of their business unit to both business leadership and the CISO.

7.2. Security Champions

Security Champions are individuals within business units or development teams who advocate for and embed security practices into their daily work. Their responsibilities include:

- **Awareness:** Raising security awareness among their peers and promoting a security-first mindset.
- **Best Practices:** Advocating for and helping implement secure coding practices, secure design principles, and other security best practices.
- **Feedback Loop:** Providing feedback from their teams to the central security function on practical challenges and opportunities for security improvement.

- **Training:** Assisting in delivering security training and guidance to their colleagues.

7.3. Department Managers

Department Managers play a vital role in ensuring that security is integrated into departmental operations and processes. Their responsibilities include:

- **Policy Enforcement:** Ensuring that departmental employees understand and adhere to security policies and procedures.
- **Asset Protection:** Protecting departmental information assets and ensuring appropriate access controls are in place.
- **Risk Management:** Identifying and managing security risks specific to their department's operations.
- **Security Training:** Ensuring that their team members receive adequate security awareness training.
- **Compliance:** Contributing to the department's compliance with security regulations and internal policies.

8. Security Committees and Working Groups

8.1. Purpose and Structure

Security committees and working groups are essential for fostering collaboration, facilitating decision-making, and ensuring broad organizational buy-in for security initiatives. Their purpose and structure include:

- **Purpose:** To provide a forum for discussing security strategy, reviewing risk posture, approving policies, overseeing major security projects, and coordinating incident response efforts.
- **Structure:** Typically composed of representatives from various departments, including IT, legal, compliance, human resources, and key business units. They may operate at different levels (e.g., executive security committee, operational security working group).
- **Frequency:** Meetings are usually held on a regular basis (e.g., monthly, quarterly), with ad-hoc meetings convened for urgent matters.

8.2. Key Committees

- **Executive Security Committee:** Composed of senior leaders, this committee provides strategic direction, approves major security investments, and reviews overall risk posture.
- **Information Security Steering Committee:** Oversees the implementation of the information security program, reviews policy effectiveness, and monitors security performance metrics.
- **Incident Response Team (IRT):** A dedicated working group responsible for managing and coordinating the response to security incidents.
- **Data Governance Committee:** Focuses on policies and procedures related to data classification, protection, and privacy, often with significant security implications.

9. Stakeholder Engagement Strategies

Effective security governance relies heavily on robust stakeholder engagement. Strategies include:

- **Clear Communication:** Tailoring security messages to different audiences, using clear, concise language, and emphasizing the business impact of security.

- **Regular Reporting:** Providing timely and relevant security reports to all stakeholders, from the board to individual employees.
- **Training and Awareness:** Implementing comprehensive security awareness programs and targeted training for specific roles.
- **Feedback Mechanisms:** Establishing channels for stakeholders to provide feedback, report concerns, and contribute to security improvements.
- **Collaboration:** Fostering a collaborative environment where security is seen as a shared responsibility rather than solely an IT function.

10. Accountability and Delegation

10.1. Establishing Accountability

Clear accountability is fundamental to effective security governance. This involves:

- **Defined Roles:** Clearly defining roles and responsibilities for all security-related activities.
- **Performance Metrics:** Establishing measurable performance metrics for security objectives and holding individuals and teams accountable for achieving them.
- **Reporting Lines:** Ensuring clear reporting lines for security incidents, risks, and compliance issues.
- **RACI Matrix:** Utilizing a RACI (Responsible, Accountable, Consulted, Informed) matrix to clarify roles for specific tasks and decisions.

10.2. Delegation of Authority

Effective delegation of authority ensures that security decisions can be made efficiently at appropriate levels. This includes:

- **Empowerment:** Empowering individuals and teams with the authority necessary to execute their security responsibilities.
- **Guidelines:** Providing clear guidelines and frameworks for delegated decision-making.
- **Oversight:** Maintaining appropriate oversight mechanisms to ensure delegated authority is exercised responsibly and in alignment with organizational objectives.

11. Role Conflicts and Separation of Duties

11.1. Identifying Role Conflicts

Role conflicts can arise when an individual or department has responsibilities that could create a conflict of interest, potentially compromising security. Common conflicts include:

- **Development vs. Security Testing:** Developers testing their own code for security vulnerabilities.
- **Operations vs. Security Monitoring:** Operations teams responsible for both system uptime and security monitoring of those systems.
- **Administration vs. Audit:** Individuals with administrative access also responsible for auditing their own activities.

11.2. Implementing Separation of Duties (SoD)

Separation of Duties (SoD) is a critical control designed to prevent fraud, errors, and unauthorized actions by requiring multiple individuals to complete a critical task. Key aspects include:

- **Segregation of Functions:** Dividing critical tasks into distinct components, each performed by a different individual or team.
- **Least Privilege:** Granting individuals only the minimum access necessary to perform their job functions.
- **Rotation of Duties:** Periodically rotating responsibilities among employees to reduce the risk of collusion and detect potential issues.
- **Independent Review:** Ensuring that critical activities are subject to independent review and approval.

12. Governance Documentation

Comprehensive and accessible documentation is vital for maintaining a robust security governance framework. Key documentation includes:

- **Security Policies:** High-level statements outlining the organization's stance on information security.
- **Security Standards:** Mandatory requirements that support security policies and provide specific controls.
- **Security Procedures:** Detailed, step-by-step instructions for implementing security controls and performing security-related tasks.
- **Security Baselines:** Minimum security configurations for systems and applications.
- **Risk Management Framework:** Documentation outlining the organization's approach to identifying, assessing, and treating risks.
- **Incident Response Plan:** A detailed plan for responding to security incidents.
- **Security Committee Charters:** Documents defining the purpose, scope, membership, and responsibilities of security committees.
- **Roles and Responsibilities Matrix:** A detailed matrix mapping specific security tasks to responsible roles (e.g., RACI matrix).

Regular review and updates of all governance documentation are essential to ensure its continued relevance and accuracy.

13. Case Studies

Case Example: Failure to Appoint a DPO

Imagine an organization that, despite being legally required to appoint a DPO, either fails to do so, appoints someone without the necessary expertise or independence, or does not provide them with adequate resources or authority. This isn't a hypothetical scenario; it's a common compliance pitfall with severe consequences. Let's explore these consequences in detail:

Regulatory Fines and Sanctions

Regulators are increasingly imposing fines specifically for the failure to appoint a DPO or for appointing one who doesn't meet the legal requirements. These fines can be substantial, signaling the seriousness with which authorities view this role. For example, under GDPR, fines for non-compliance with DPO requirements can be up to €10 million or 2% of the organization's total worldwide annual turnover, whichever is higher. This is a direct financial hit that can significantly impact profitability.

Lack of Internal Guidance and Expertise

Without a dedicated DPO, the organization lacks a central point of contact and expertise for data protection matters. Employees may not know who to turn to with questions about data handling, leading to inconsistent practices and increased risk of breaches. This can manifest as:

- **Ad-hoc decision-making:** Departments making privacy-related decisions without proper guidance.
- **Missed opportunities for privacy-by-design:** New products or services being developed without privacy considerations built in from the start.
- **Increased training burden:** Without a DPO to lead privacy training, employees may receive inadequate or inconsistent information.

Ineffective Compliance Monitoring

The DPO is crucial for monitoring an organization's compliance with data protection laws. Without this oversight, the organization might unknowingly be engaging in non-compliant activities, only discovering issues after a breach or regulatory investigation. This proactive monitoring is essential for identifying and rectifying issues before they escalate. Without it, the organization is essentially operating blind, hoping for the best.

Eroding Trust and Reputational Damage

When an organization fails to meet fundamental regulatory requirements like appointing a DPO, it signals a lack of commitment to data protection. This can erode trust among customers, partners, and even employees, who may perceive the organization as irresponsible with their personal data. News of regulatory non-compliance can quickly spread, leading to significant reputational damage that is difficult and costly to repair. In today's data-driven economy, trust is a critical currency, and a failure in this area can have long-lasting negative impacts on brand image and customer loyalty.

Increased Legal Exposure and Liabilities

The absence of a DPO can weaken an organization's defense in the event of a data breach or privacy complaint. It demonstrates a failure to implement a key safeguard mandated by law, potentially leading to greater legal liabilities. Affected individuals may pursue civil lawsuits, and regulators may impose additional sanctions for systemic failures in governance. This can result in costly legal battles, settlements, and a prolonged period of legal uncertainty.

This example of the DPO underscores a broader principle in security governance: simply having a framework or a list of roles isn't enough. These roles must be actively filled by competent individuals, empowered with the necessary authority and resources, and integrated effectively into the organization's overall governance structure. The failure to do so creates significant vulnerabilities and can lead to severe consequences, not just in terms of fines, but also in terms of reputation, operational disruption, and legal exposure.

14. Summary

Effective security governance is a continuous and evolving process that requires a clear understanding and diligent execution of roles and responsibilities across all levels of an organization. By establishing robust governance structures, defining clear roles, fostering strong leadership, engaging all stakeholders, and maintaining comprehensive documentation, organizations can significantly enhance their security posture, manage risks effectively, and ensure compliance with regulatory requirements. The dynamic nature of cyber threats necessitates an adaptive approach to security governance, emphasizing continuous improvement and a culture where security is a shared responsibility.

15. References

ISO/IEC 27014:2020 - Information security, cybersecurity and privacy protection Governance of information security. International Organization for Standardization.

ISACA. (2019). COBIT 2019 Framework: Introduction and Methodology. ISACA.

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.

The Institute of Internal Auditors. (2020). The IIA's Three Lines Model: An update of the Three Lines of Defense.

Fitzgerald, T. (2020). CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers. CRC Press.

Axelos. (2019). ITIL 4 Foundation: ITIL 4 Edition. The Stationery Office.

Maymi, F. J., & Harris, S. (2018). CISSP All-in-One Exam Guide, Eighth Edition. McGraw-Hill Education.

Kouns, J., & Minoli, D. (2011). Information Technology Risk Management in Enterprise Environments. Wiley.

Whitman, M. E., & Mattord, H. J. (2021). Management of Information Security, 6th Edition. Cengage Learning.

Swanson, M., & Bowen, P. (2006). NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers. National Institute of Standards and Technology.

ISO/IEC 27014:2020 - Information security, cybersecurity and privacy protection — Governance of information security. International Organization for Standardization.

ISACA. (2019). COBIT 2019 Framework: Introduction and Methodology. ISACA.

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.

The Institute of Internal Auditors. (2020). The IIA's Three Lines Model: An update of the Three Lines of Defense.

Fitzgerald, T. (2020). CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers. CRC Press.

Axelos. (2019). ITIL 4 Foundation: ITIL 4 Edition. The Stationery Office.

Maymi, F. J., & Harris, S. (2018). CISSP All-in-One Exam Guide, Eighth Edition. McGraw-Hill Education.

Kouns, J., & Minoli, D. (2011). Information Technology Risk Management in Enterprise Environments. Wiley.

Whitman, M. E., & Mattord, H. J. (2021). Management of Information Security, 6th Edition. Cengage Learning.

Swanson, M., & Bowen, P. (2006). NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers. National Institute of Standards and Technology.