SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Program Strategy & Operations > Strategic Planning/Management >

Building a Comprehensive Security Governance Framework for Today's Businesses

Corporate Security Governance

The focus of enterprise risk management (ERM) has expanded over the years with concerns for ethical and reputational risk, employee safety, cyber and business continuity risk, and threats of terrorism.

These expanded areas of concern for corporate boards have pushed Security programs to provide a wider array of internal controls that support the assurance of effective governance practices that guide corporate strategy and operations.

A mature corporate security program will have a framework for security governance that drives adherence to corporate security programs and reduces external risk by ensuring compliance with company standards and policies.

The primary tenets of a security governance program include:

- an operational risk leadership advisory council
- security policies
- risk-based security standards and regulations

- an assessment and audit program
- metrics for measuring adoption and enforcement of the governance program.

Operational Risk Leadership Advisory Council

Despite its expanding compliance and governance scope, Corporate Security does not typically have a seat at the Enterprise Risk Management (ERM) table. This limits board-level consideration of operational risks. In addition to ERM, a governance strategy can benefit from the creation of an Operational Risk Leadership Advisory Council (ORLAC).

This council is different from the board-level ERM committee that oversees and manages risks that could impact the firm’s reputation in the market and ability to achieve its objectives. An ORLAC is a chartered or codified, cross-functional governance body that reports to the ERM committee and enables, facilitates, and prioritizes the organization's *operational* risk management.

This council allows operational leaders to collaborate at a high level to inform and advise enterprise risk strategy. Participating functions vary but could include Corporate and Cyber Security, IT, Legal, HR, Internal Audit, Risk, Supply Chain, EH&S, or Procurement. Each of these members brings their own view of operational risks, best practices and performance standards, yielding a more integrated perspective on risk and the role of governance in mitigation strategy.

A council like this offers a vehicle to enable, facilitate and prioritize the organization's operational risk management strategy and to identify and remove redundancies based on risk exposures and threat priorities. It also provides a place for business leaders and section chiefs to cross-functionally evaluate, prioritize and resource mitigation options for both emerging and residual threats.

It enables the organization to confront external and internal risk factors that require collaborative, continuous, and nimble processes, and it can assist in detecting emerging and fast-onset risks, especially at the operational levels.

While enterprise risk management and operational risk management arguably remain two distinct lenses for risk management, their combined processes and capabilities enable higher levels of integrated risk mitigation assurance and confidence.

Security Policies

A strong policy can make a significant impact on security’s ability to set, communicate, and enforce requirements for managing risk.

Security organizations should maintain written documentation of controls and requirements detailing how the enterprise will mitigate the security risks identified as a priority by the business. The organization should define the hierarchy and subordinate relationships between the various specifications, policies, and operating procedures (SOP) authored at different levels of the company.

It's important to include stakeholders that are involved in development prior to drafting. Make sure policy documents have clearly defined owners and state their scope and objectives in the opening pages. Also include the list of stakeholders involved in the policy's enforcement. Providing clear context and minimizing ambiguity helps to avoid misinterpretation and clarifies the expectations and obligations of stakeholders to address the security risks of concern.

To avoid confusion, minimize the use of technical terminology that may be unfamiliar to individuals outside the organization, unless they are defined in a dedicated glossary section.

To make policies easy to find, consider keeping them in a searchable database that is access controlled and available to employees and suppliers on a need-to-know basis.

Use a standardized format including a naming convention, document numbering and version sequencing. Include a schedule for policy review and a change control log to show version history, release dates, and a short description of the updates made in each subsequent release

Include an "escalations" clause which describes the process for exceptions, appeals, and consequences for repeated violations or non-compliance.

Develop a plan to effectively communicate the new policy as it takes effect, and ensure that communication is accompanied by appropriate training.

Risk-based Security Standards

Ensure the security program is compliant with all security-related laws, regulations and standards that are associated with your industry. Some regulations are applicable to most publicly traded companies and others are industry specific. Some examples:

- Food Safety Modernization Act 21 U.S. Code § 350g
- MARSEC - Maritime Transportation Act
- NERC-CIP - NERC Reliability Standards - Critical Infrastructure Protection
- Foreign Corrupt Practices Act
- BASEL III
- EU General Data Protection Regulation

Beyond regulation, there is an extensive foundation of accepted standards and guidelines that directly or indirectly touch on corporate security. A few examples:

- ISO 37000:2021 - Governance of Organizations (reputational and insider risk, codes of conduct, behavioral ethics, background vetting)

- ISO 22301:2019 - Security and Resilience - Requirements for Business Continuity Management Systems
- ISO/IEC 27002:2022 - Information Security (includes chapters on physical and people controls)
- ISO 31030:2021 - Travel Risk Management
- ISO 28000 - Security Management Systems - Requirements (including supply chain security)
- NFPA 1660 (2023) - Standard for Emergency, Continuity, and Crisis Management: Preparedness, Response, and Recovery
- NFPA 730 (2023) - Guide for Premises Security
- NFPA 3000 - Active Shooter/Hostile Event Response

Applying industry standards can make benchmarking against peer companies easier. Additionally, should the organization choose to seek full certification or outside validation of conformance to industry standards, such accreditations can serve as a powerful signal to customers and can be a differentiator that provides a recognized measure of security assurance. Adoption of external security standards may also benefit the organization's position with some insurance carriers, demonstrating a commitment to risk mitigation practices through an accredited and recognized framework.

Organizations may choose to adapt or align their internal policies to industry security standards as well. Mirroring industry standards bolsters the credibility of the organization's internal requirements and demonstrates the rationale and justification for controls.

Ensuring alignment with external standards becomes particularly important when managing third-party risk from suppliers and partners. Sourcing and procurement departments may choose to require suppliers to demonstrate certification or conformance to industry security standards as a contingency for any business award. Suppliers who demonstrate current membership or security certification from an accredited body can be expedited through the due diligence and vetting process, having already proven their commitment to managing enterprise security risks.

Assessment and Audit Program

Under ideal circumstances, a firm will establish an independent internal audit organization that resides outside all core business functions and reports directly to an executive-level leader. For corporate security, the audit team can assess security risk assessment results, mitigation controls, processes, procedures, and systems to ensure they are protecting corporate assets and are aligned with business goals. Audit results can be used to improve the security function by identifying vulnerabilities, potential risks, noncompliance and areas for improvement for security.

Additionally, organizations may establish a separate group solely responsible for auditing their third-party supplier's compliance to security policies. Preferably, this group will comprise members with technical knowledge of the business unit's operational goals and objectives. External supplier assessments should be risk-based and should consider multiple inherent risk factors such as geographic location, foreign ownership and control, commodity type, and operational dependency when determining which suppliers to include and why.

Metrics for Measuring Adoption and Enforcement

Establish a series of metrics and indicators to measure the overall health and performance of the security governance program. Include these metrics in the security risk management policy, describing which data is used and the formula behind how the metric will be scored.

All metrics data should originate from an agreed-upon source, derived from a system of record already used and recognized within the enterprise. Metrics should be included in supplier contracts and used when awarding new contracts projects.

Emerging Topics in Security Governance

While the above tenets outline traditional security governance, it's also important to consider emerging factors that are influencing organizations today.

The Role of AI and Automation in Security Governance. As security threats grow more sophisticated, AI and automation have become essential components of modern security governance. Machine learning algorithms can identify potential risks in real time, while automation streamlines tasks such as compliance checks and log reviews. These technologies enhance efficiency and enable faster, data-driven decision-making.

Addressing Hybrid Work Environments in Risk Policies. The shift to hybrid work environments introduces new challenges, such as securing home networks, managing endpoint devices, and mitigating insider threats. Consider expanding risk policies to address these issues, ensuring security in decentralized workforces through identity management solutions and clear guidelines.

Integrating ESG Metrics into Security Programs. Security governance increasingly intersects with Environmental, Social, and Governance (ESG) criteria. By integrating ESG metrics into security programs, organizations can enhance transparency, meet regulatory requirements, and appeal to socially conscious stakeholders. ESG-aligned governance demonstrates a commitment to ethical, sustainable business practices.

Good security governance provides a structural, reliable, and consistent approach to managing security risks. Businesses should evaluate their existing programs and integrate forward-looking strategies to remain effective and competitive.

Contributors: George Campbell, Mark Kelly, Kathleen Kotwica

Visit the Security Executive Council web site to view more resources in the Security Program Strategy & Operations : Strategic Planning/Management series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/