Corporate Security Governance and Compliance Frameworks Training Course



26 - 30 Oct 2026

Milan

5900 € (Per Person)

Ref: #SM4714_131188

Course Introduction / Overview:

In today's hyper-connected digital landscape, establishing a robust corporate security governance and compliance framework is no longer a strategic advantage but a fundamental necessity for survival and growth. This course provides a comprehensive exploration of the principles, frameworks, and practices required to build and maintain an effective security posture that aligns with business objectives and regulatory mandates. As highlighted by security expert Eugene H. Spafford, effective security is not just about technology but about well-defined policies and governance. This program delves into this philosophy, moving beyond technical controls to address the strategic integration of security into the corporate fabric. Participants will learn to navigate the complex web of international standards like ISO 27001 and frameworks such as NIST and COBIT, transforming compliance from a burdensome cost center into a value-driven business enabler. BIG BEN Training Center has designed this immersive experience to equip leaders with the skills to architect, implement, and manage security governance systems that protect critical assets, ensure regulatory adherence, and build stakeholder trust in an era of persistent cyber threats.

Target Audience / This training course is suitable for:

- Chief Information Security Officers (CISOs) and security executives.
- IT Security Managers and Directors.
- Compliance and Privacy Officers.
- Internal and External Auditors.
- Risk Management Professionals.
- Legal Counsel and Corporate Governance Specialists.
- IT Managers and System Administrators.
- Senior Business Leaders and Board Members with security oversight.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Information Technology and Telecommunications.
- Government and Public Sector Agencies.
- Energy, Oil, and Gas.
- Retail and E-commerce.
- Manufacturing and Industrial Control Systems.
- Consulting and Professional Services.

Target Organizations Departments:

- Information Technology (IT) and Information Security.
- Legal and Compliance.
- Internal Audit.
- Risk Management.
- Corporate Governance.
- Operations Management.
- Human Resources.
- Procurement and Vendor Management.

Course Offerings:

By the end of this course, the participants will have able to:

- Develop a comprehensive corporate security governance strategy aligned with business goals.
- Select, adapt, and implement internationally recognized security frameworks like ISO 27001 and NIST.
- Conduct thorough risk assessments and establish a formal risk management program.
- Design and enforce effective information security policies, standards, and procedures.
- Establish key performance indicators (KPIs) and metrics to measure security effectiveness.
- Navigate complex legal and regulatory compliance requirements such as GDPR and CCPA.
- Prepare for and manage internal and external security audits successfully.
- Communicate security risks and strategies effectively to executive leadership and the board.
- Integrate security governance into the entire organizational lifecycle, from procurement to operations.
- Develop a robust incident response and business continuity governance structure.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, practical, and engaging, ensuring participants can translate theoretical knowledge into real-world application. This course moves beyond traditional lectures, employing a blended learning approach that includes expert-led presentations, in-depth case study analyses of real corporate security breaches and successes, and collaborative group workshops. Participants will engage in hands-on exercises, such as developing a draft security policy, conducting a mock risk assessment, and creating a board-level security report. Interactive sessions, facilitated discussions, and peer-to-peer knowledge sharing are central to the learning experience, allowing attendees to explore diverse perspectives and solve complex governance challenges together. Continuous feedback is provided by the instructor to guide learning and reinforce key concepts. This immersive and practical approach ensures that participants leave not just with knowledge, but with the confidence and skills to implement and enhance security governance and compliance frameworks within their own organizations.

Course Agenda (Course Units):

Unit One: Foundations of Corporate Security Governance

- Introduction to Corporate Security Governance, Risk, and Compliance (GRC).
- The critical role of governance in mitigating cyber threats and business risks.
- Understanding the legal, regulatory, and ethical landscape of information security.
- Key principles of information security management.
- Aligning security strategy with overall business objectives and corporate culture.
- Roles and responsibilities in security governance from the board to operations.
- Establishing a formal charter and mandate for the security function.

Unit Two: Key Governance and Compliance Frameworks

- Deep dive into ISO/IEC 27001 and the Information Security Management System (ISMS).
- Exploring the NIST Cybersecurity Framework (CSF) for critical infrastructure.
- Understanding the COBIT framework for IT governance and management.
- Comparing and contrasting major frameworks to select the right fit.
- Adapting and tailoring frameworks to specific organizational needs and industry regulations.
- Introduction to data privacy regulations like GDPR and CCPA.
- Mapping controls across multiple compliance requirements to reduce redundancy.

Unit Three: Implementing the Security Governance Program

- Developing a strategic roadmap for security governance implementation.
- Crafting effective and enforceable information security policies and standards.
- Conducting comprehensive security risk assessments and analysis.
- Implementing a robust risk treatment and mitigation plan.
- Designing and deploying essential security controls.
- Building a security-aware culture through training and awareness programs.
- Managing third-party and supply chain security risks.

Unit Four: Measurement, Monitoring, and Auditing

- Defining and tracking Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs).
- Developing a security metrics and reporting program for different stakeholders.
- Techniques for continuous security monitoring and improvement.
- Planning and executing internal and external security audits.
- Managing audit findings and implementing corrective action plans.
- The role of governance in incident response and crisis management.
- Integrating business continuity and disaster recovery planning into the governance framework.

Unit Five: Advanced Governance and Strategic Leadership

- Communicating security value and risk to the Board of Directors and executive management.
- Budgeting for and demonstrating the return on investment (ROI) of security initiatives.
- Governing emerging technologies like cloud computing, AI, and IoT.
- Navigating the complexities of cyber insurance and corporate liability.
- The future of security governance and anticipating future trends.
- Building a mature and resilient security governance program.
- Final project workshop: Developing a high-level governance framework for a case study organization.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

How can an organization design a security governance framework that is robust enough to mitigate evolving cyber threats without stifling the innovation and agility required for competitive growth?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by adopting a holistic, business-centric approach to security governance, moving beyond a purely technical or compliance-driven perspective. While many programs focus on the specifics of a single framework, this training provides a comparative analysis, equipping participants with the critical thinking skills to select, blend, and tailor frameworks to their unique organizational context. A key differentiator is the strong emphasis on strategic communication. We dedicate significant time to mastering the art of translating complex security risks and metrics into clear, compelling business language for executive leadership and boards of directors, a skill crucial for securing buy-in and resources. The curriculum is built around practical application, using real-world case studies and hands-on workshops to bridge the gap between theory and implementation. Rather than simply learning what a policy should contain, participants will draft one. Instead of just discussing risk assessment, they will perform one. This focus on actionable skills ensures that attendees return to their organizations not just as more knowledgeable professionals, but as effective leaders capable of building and managing a truly resilient security governance program.