Strategic Cybersecurity Governance and Risk Oversight Training Course



28 Dec 2026 - 01 Jan 2027

Lisbon

4500 € (Per Person)

Ref: #GRC8858_166101

Course Introduction / Overview:

In today's hyper-connected digital landscape, cybersecurity has transcended its traditional IT boundaries to become a critical component of corporate governance and strategic risk management. This course provides a comprehensive framework for establishing and overseeing a robust cybersecurity governance program. It moves beyond technical jargon to address the strategic imperatives that boards of directors, C-suite executives, and senior managers must command. We will explore the principles articulated by thought leaders like Eugene H. Spafford, who emphasizes a holistic approach to security. The curriculum is designed to equip leaders with the knowledge to effectively challenge, guide, and support their organization's cybersecurity posture. Drawing from concepts found in seminal works such as "Cybersecurity and Cyberwar: What Everyone Needs to Know", this program delves into creating resilient governance structures, managing cyber risk as a business risk, and ensuring regulatory compliance. BIG BEN Training Center has developed this course to bridge the gap between technical security teams and executive leadership, fostering a common language and a unified strategy for protecting critical assets and ensuring business continuity in the face of evolving cyber threats.

Target Audience / This training course is suitable for:

- Board Members and Directors.
- Chief Executive Officers (CEOs).
- Chief Information Security Officers (CISOs).
- Chief Risk Officers (CROs).
- IT Directors and Senior IT Managers.
- Compliance and Legal Officers.
- Internal and External Auditors.
- Senior Business Leaders with risk oversight responsibilities.
- Corporate Governance Professionals.

Target Sectors and Industries:

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

Target Organizations Departments:

- Executive Leadership and Board of Directors.
- Information Technology (IT) and Information Security.
- Risk Management.
- Legal and Compliance.
- Internal Audit.
- Corporate Strategy and Planning.
- Operations Management.
- Finance and Accounting.

Course Offerings:

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

- Develop and implement a comprehensive cybersecurity governance framework.
- Align cybersecurity strategy with overall business objectives and risk appetite.
- Effectively oversee and challenge the organization's cyber risk management practices.
- Understand the roles and responsibilities of the board and senior management in cybersecurity.
- Interpret and apply key industry standards like NIST, ISO 27001, and COBIT.
- Establish meaningful metrics and key risk indicators (KRIs) for board-level reporting.
- Navigate the complex landscape of cybersecurity regulations and legal liabilities.
- Foster a strong, security-aware culture throughout the organization.
- Evaluate and manage third-party and supply chain cyber risks.
- Lead strategic incident response planning and crisis management efforts.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and highly practical. We believe that effective learning in cybersecurity governance comes from applying concepts to real-world scenarios. The course heavily utilizes a case-study approach, where participants will analyze actual cyber incidents and governance failures to extract actionable lessons. Interactive sessions, including group discussions, tabletop exercises, and simulated board meetings, will challenge participants to make critical decisions under pressure. Our expert instructors facilitate a collaborative learning environment, encouraging the sharing of experiences and diverse perspectives. Participants will work in teams to develop a cybersecurity governance charter and a board-level reporting dashboard for a fictional corporation. This hands-on approach ensures that the theoretical knowledge gained is immediately translated into practical skills. Continuous feedback is provided throughout the course, allowing participants to refine their understanding and approach. This blend of instruction, collaboration, and application ensures a rich and impactful learning experience that extends far beyond the classroom.

Course Agenda (Course Units):

Unit One: Foundations of Cybersecurity Governance

- Defining cybersecurity governance and its distinction from management.
- The critical role of the board and executive leadership in cyber oversight.
- Understanding the modern threat landscape and its business implications.
- Key governance principles: accountability, strategy, and assurance.
- Introduction to leading frameworks: NIST Cybersecurity Framework (CSF).
- Exploring the ISO 27001 standard for Information Security Management Systems (ISMS).
- Aligning cybersecurity initiatives with strategic business goals.

Unit Two: Strategic Cyber Risk Management

- Integrating cyber risk into the enterprise risk management (ERM) framework.
- Methodologies for risk identification, assessment, and analysis.
- Defining and communicating the organization's risk appetite and tolerance.
- Developing effective risk treatment and mitigation strategies.
- Implementing a continuous risk monitoring and reporting process.
- The role of threat intelligence in proactive risk management.
- Quantitative vs. qualitative risk assessment techniques.

Unit Three: Legal, Regulatory, and Compliance Landscape

- Navigating the global web of cybersecurity laws and regulations (e.g., GDPR, CCPA).
- Understanding industry-specific compliance requirements (e.g., HIPAA, PCI DSS).
- The legal duties and potential liabilities of directors and officers.
- Managing data privacy and data protection governance.
- Contractual considerations for cybersecurity in third-party agreements.
- Developing a defensible compliance and ethics program.
- Responding to regulatory inquiries and investigations.

Unit Four: Board-Level Reporting and Building a Security Culture

- Designing effective cybersecurity dashboards and metrics for the board.
- Communicating technical risks in clear, business-oriented language.
- Establishing key performance indicators (KPIs) and key risk indicators (KRIs).
- The CISO's role in advising and reporting to the board.
- Strategies for fostering a pervasive, top-down cybersecurity culture.
- Implementing security awareness and training programs for all employees.
- Measuring the effectiveness of cultural and awareness initiatives.

Unit Five: Advanced Governance and Future-Proofing Strategy

- Oversight of incident response and business continuity planning.
- Managing cybersecurity in mergers and acquisitions (M&A) due diligence.
- Third-party and supply chain risk governance.
- Addressing emerging technology risks: AI, IoT, and cloud security.
- The function of cybersecurity audit and independent assurance.
- Developing a long-term cyber resilience strategy.
- Framework for continuous improvement of the cybersecurity governance program.

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:

Beyond compliance checklists, how can an organization's leadership truly embed a proactive, risk-aware cybersecurity culture that permeates every level of the business?

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

This course distinguishes itself by focusing squarely on the strategic and oversight dimensions of cybersecurity, a perspective often neglected in technically-focused or purely compliance-driven training. While other courses may teach the "what" of security controls, we emphasize the "why" and "how" from a leadership viewpoint. Our curriculum is specifically designed for the boardroom and the C-suite, translating complex technical concepts into the language of business risk, strategy, and value preservation. The program's uniqueness lies in its heavy reliance on strategic simulations and board-level tabletop exercises, which move beyond passive learning to active decision-making. Participants do not just learn about governance frameworks; they practice applying them in realistic crisis scenarios. Furthermore, the course content is forward-looking, addressing not only current threats and regulations but also the governance challenges posed by emerging technologies like artificial intelligence and the Internet of Things. It provides a holistic, integrated view of cyber risk, connecting it to enterprise risk management, corporate strategy, and organizational culture in a way that few other programs do.