Advanced Cyber Security Governance and Risk Management Training Course



16 - 20 Nov 2026

Rome

5800 € (Per Person)

Ref: #CYB3997_87725

Course Introduction / Overview:

In today's hyper-connected digital landscape, cybersecurity has transcended its traditional role as a technical IT function to become a critical component of corporate governance and strategic business planning. This advanced course is meticulously designed to equip leaders and professionals with the strategic foresight and practical skills needed to build and manage a robust cybersecurity governance and risk management program. We will move beyond basic security protocols to explore the intricate relationship between technology, risk, compliance, and business objectives. Drawing on foundational principles discussed by experts like Eugene H. Spafford and in seminal texts such as "Managing Information Security," this program provides a comprehensive GRC (Governance, Risk, and Compliance) perspective. Participants will learn to establish clear lines of authority, define risk appetite, and implement control frameworks that are not only effective but also aligned with organizational goals. At BIG BEN Training Center, we provide a holistic learning experience that empowers you to lead cybersecurity initiatives, communicate effectively with executive boards, and foster a resilient security culture that protects assets and enables growth in an era of persistent cyber threats.

Target Audience / This training course is suitable for:

- Chief Information Security Officers (CISOs) and aspiring security leaders.
- IT Directors and Managers.
- Cybersecurity Analysts and Consultants.
- Risk Management Professionals.
- Compliance Officers and Managers.
- Internal and External Auditors.
- IT Governance Professionals.
- Legal Counsel involved in data privacy and security.
- Business executives seeking to understand cyber risk.

Target Sectors and Industries:

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

Target Organizations Departments:

- Information Technology (IT).
- Information Security and Cybersecurity.
- Risk Management.
- Internal Audit.
- Legal and Compliance.
- Corporate Governance.
- Executive Management.
- Operations.

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 overarching business objectives and goals.
- Conduct advanced cyber risk assessments using qualitative and quantitative methods.
- Establish and manage an effective information security risk management program.
- Navigate the complex landscape of global and local cybersecurity regulations.
- Master the principles of major security frameworks like NIST, ISO 27001, and COBIT.
- Design and implement robust security policies, standards, and procedures.
- Communicate cyber risk effectively to executive leadership and the board of directors.
- Develop key performance indicators (KPIs) and key risk indicators (KRIs) for cybersecurity.
- Lead incident response planning and crisis management from a governance perspective.
- Evaluate and manage third-party and supply chain cyber risks.

Course Methodology:

This training course at BIG BEN Training Center employs a dynamic and interactive learning methodology designed for maximum knowledge retention and practical application. We believe that adult learning is most effective when it is engaging, relevant, and hands-on. The curriculum is delivered through a blend of expert-led presentations, in-depth discussions, and collaborative group activities. Participants will analyze real-world case studies of major security breaches and governance failures, dissecting the root causes and debating effective mitigation strategies. Interactive workshops will guide attendees through the process of building key program components, such as a risk register, a policy framework, and a board-level report. Team-based exercises will simulate risk assessment and incident response scenarios, requiring participants to work together to make critical decisions under pressure. Throughout the course, there will be ample opportunity for peer-to-peer learning and direct interaction with the instructor, who will provide personalized feedback and facilitate a rich exchange of ideas and experiences. Our approach ensures that participants leave not just with theoretical knowledge, but with the confidence and practical tools to implement effective cybersecurity governance and risk management in their own organizations.

Course Agenda (Course Units):

Unit One: Foundations of Cybersecurity Governance

- The strategic importance of cybersecurity governance.
- Distinguishing between governance, management, and operations.
- Core principles of information security governance.
- Key roles and responsibilities (Board, C-Suite, CISO).
- Introduction to major governance frameworks (COBIT, ISO/IEC 38500).
- Aligning security initiatives with business strategy and objectives.
- Developing a business case for cybersecurity investments.
- Establishing a culture of security from the top down.

Unit Two: Implementing Governance Frameworks and Policies

- Deep dive into the NIST Cybersecurity Framework (CSF).
- Understanding the ISO 27001 Information Security Management System (ISMS).
- Developing a hierarchy of security policies, standards, and procedures.
- The policy lifecycle: creation, approval, distribution, and review.
- Defining and communicating the organization's risk appetite and tolerance.
- Establishing clear lines of authority and accountability.
- Integrating cybersecurity into the enterprise architecture.
- Metrics and reporting for governance oversight.

Unit Three: Advanced Cyber Risk Management

- The complete risk management lifecycle: identify, assess, treat, monitor, report.
- Methodologies for threat modeling and vulnerability identification.
- Qualitative vs. quantitative risk analysis techniques.
- Introduction to the Factor Analysis of Information Risk (FAIR) model.
- Developing and maintaining a comprehensive risk register.
- Risk treatment strategies: mitigation, transference, acceptance, and avoidance.
- Managing third-party and supply chain risk.
- Integrating risk management into the System Development Life Cycle (SDLC).

Unit Four: The Regulatory and Compliance Landscape

- Navigating key data privacy regulations (GDPR, CCPA).
- Industry-specific compliance requirements (PCI DSS, HIPAA).
- The role of audits in verifying compliance and control effectiveness.
- Managing internal and external audit processes.
- Contractual and legal obligations in cybersecurity.
- Evidence collection and preservation for compliance.
- Strategies for continuous compliance monitoring.
- Reporting compliance status to stakeholders.

Unit Five: Strategic Leadership, Incident Response, and Future Trends

- Developing effective cybersecurity metrics (KPIs and KRIs).
- Creating compelling reports and dashboards for the board of directors.
- Building and testing a strategic incident response plan.
- Crisis communication and management during a cyber incident.
- The role of threat intelligence in strategic planning.
- Emerging trends in cyber governance: AI, OT, and cloud security.
- Building a resilient organization for the future.
- Capstone exercise: Simulating a board-level cyber crisis meeting.

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:

As cyber threats evolve from purely technical to geopolitical weapons, how must a CISO's role transform from a technologist to a strategic business and political advisor?

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

This course distinguishes itself by adopting a strategic, business-centric perspective on cybersecurity, moving beyond the purely technical implementation of security controls. While many programs focus on the "how" of security tools, we concentrate on the "why" and "so what" from a leadership viewpoint. Our curriculum is uniquely structured to bridge the critical gap between the server room and the boardroom. We emphasize the development of soft skills essential for modern security leaders, such as communicating complex risks in simple business terms, negotiating budgets, and influencing corporate culture. The program's deep dive into quantitative risk analysis using frameworks like FAIR provides participants with a powerful tool to articulate cyber risk in financial terms, a skill highly valued by executive committees. Furthermore, the course content is not static; it incorporates forward-looking topics such as the governance of AI security and operational technology, preparing participants for the next wave of challenges. By focusing on strategic alignment, leadership, and business enablement, this training provides a holistic and immediately applicable skill set that empowers participants to function as true strategic partners within their organizations, rather than just technical gatekeepers.