Advanced Information Security Governance and Protection Training Course

16 - 20 Nov 2026

Milan

5900 € (Per Person)

Ref: #DM1220_91121

Course Introduction / Overview:

In an era where data is the most valuable corporate asset, establishing a robust framework for its governance and protection is no longer optional but a fundamental business imperative. This course provides a comprehensive exploration of the principles, frameworks, and best practices of information security governance. It moves beyond purely technical controls to address the strategic alignment of security with business objectives, a concept thoroughly explored by experts like Eugene H. Spafford. Participants will delve into the core components of a successful governance program, including risk management, policy development, compliance adherence, and performance measurement. Drawing from established methodologies found in works such as "Information Security Governance: A Practical Guide for IT Managers," this program equips leaders to build and manage a resilient security posture. BIG BEN Training Center has designed this course to empower professionals to make informed decisions, effectively communicate risk to stakeholders, and cultivate a security-conscious culture throughout their organization, ensuring that security functions as a business enabler rather than a barrier. This training is essential for anyone tasked with safeguarding critical information assets and ensuring organizational resilience against evolving cyber threats.

Target Audience / This training course is suitable for:

- Information Security Managers and Directors.
- IT Managers and Team Leaders.
- Chief Information Security Officers (CISOs).
- Risk and Compliance Officers.
- IT Auditors and Consultants.
- Data Protection Officers (DPOs).
- Business Continuity Planners.
- Senior System and Network Administrators.
- Project Managers overseeing IT initiatives.
- Legal professionals specializing in technology and data privacy.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Telecommunications and Technology.
- Government Agencies and Public Sector Bodies.
- Energy and Utilities.
- Retail and E-commerce.
- Consulting and Professional Services.
- Education and Research Institutions.

Target Organizations Departments:

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

Course Offerings:

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

- Develop and implement a comprehensive information security governance framework.
- Align security strategies with overarching business goals and objectives.
- Conduct thorough risk assessments and formulate effective risk treatment plans.
- Design and enforce robust security policies, standards, and procedures.
- Navigate complex legal, regulatory, and contractual compliance requirements.
- Establish key performance indicators (KPIs) to measure security effectiveness.
- Lead incident response and business continuity planning efforts.
- Communicate security risks and strategies effectively to executive leadership.
- Foster a strong, organization-wide culture of security awareness.
- Evaluate and manage third-party and supply chain security risks.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, immersive, and practical, ensuring participants can translate theoretical knowledge into actionable skills. Our approach moves beyond traditional lectures to foster a dynamic learning environment. The course heavily relies on real-world case studies, allowing participants to analyze complex security governance challenges and dissect successful strategies from various industries. Collaborative group exercises and workshops are central to the learning process, encouraging peer-to-peer knowledge sharing and problem-solving. Participants will engage in hands-on activities such as developing a draft security policy, conducting a mock risk assessment, and outlining an incident response plan. Expert instructors facilitate discussions, providing personalized feedback and guiding participants through complex concepts. The methodology emphasizes critical thinking and strategic decision-making, preparing attendees to implement and manage effective information security governance frameworks within their own organizations. This blend of expert instruction, practical application, and interactive engagement ensures a deep and lasting understanding of the subject matter.

Course Agenda (Course Units):

Unit One: Foundations of Information Security Governance

- Introduction to Information Security Governance Principles.
- The Relationship Between Governance, Risk, and Compliance (GRC).
- Key Governance Frameworks (COBIT, ISO/IEC 27001, NIST Cybersecurity Framework).
- Defining Roles and Responsibilities in Security Governance.
- Aligning Security Strategy with Business Objectives.
- The Role of the Board of Directors and Senior Management.
- Developing a Business Case for Security Investments.

Unit Two: Strategic Risk Management and Assessment

- Principles of Information Security Risk Management.
- Risk Identification Techniques and Threat Modeling.
- Qualitative and Quantitative Risk Analysis Methods.
- Risk Evaluation and Prioritization.
- Developing a Risk Treatment and Mitigation Plan.
- Implementing and Monitoring Risk Controls.
- Creating and Maintaining a Risk Register.

Unit Three: Policy Development and Regulatory Compliance

- Crafting an Information Security Policy Hierarchy.
- Developing Effective Standards, Procedures, and Guidelines.
- Key Components of an Acceptable Use Policy (AUP).
- Navigating the Global Regulatory Landscape (GDPR, HIPAA, PCI DSS).
- Data Classification and Handling Policies.
- Managing Compliance and Preparing for Audits.
- Policy Lifecycle Management and Communication Strategies.

Unit Four: Security Operations and Incident Management

- Establishing a Security Operations Center (SOC) Framework.
- Developing a Proactive Incident Response Plan.
- Incident Detection, Triage, and Analysis.
- Containment, Eradication, and Recovery Strategies.
- Post-Incident Analysis and Lessons Learned.
- Business Continuity and Disaster Recovery Planning.
- Managing Third-Party and Supply Chain Security Risks.

Unit Five: Leadership, Metrics, and Security Culture

- Measuring and Reporting Security Performance with KPIs and KRIs.
- Creating Effective Security Dashboards for Executive Leadership.
- Building and Sustaining a Security-Aware Culture.
- Implementing Security Awareness and Training Programs.
- Ethical Considerations in Information Security.
- Future Trends in Security Governance (Cloud, AI, IoT).
- Capstone Exercise: Developing a Governance Roadmap.

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 effectively balance the need for stringent security governance with the demand for business agility and innovation?

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

This training course distinguishes itself by focusing on the strategic integration of information security within the broader context of business leadership and corporate governance. While many courses concentrate solely on the technical implementation of security controls, our curriculum emphasizes the "why" behind the "what". We equip participants with the skills to function as strategic business partners who can articulate risk in financial and operational terms, thereby securing executive buy-in and appropriate resources. The program's unique value lies in its holistic approach, bridging the gap between the server room and the boardroom. We delve deeply into the nuances of policy creation, regulatory navigation, and the art of building a pervasive security culture, which are often overlooked in technically-focused training. By integrating frameworks like COBIT and NIST not just as compliance checklists but as tools for strategic alignment, participants learn to build security programs that are resilient, adaptable, and directly supportive of organizational goals. This course is designed for current and future leaders who understand that effective security governance is a critical driver of business success and competitive advantage.