Strategic Information Security Governance and Risk Training Course



02 - 06 Nov 2026

Milan

5900 € (Per Person)

Ref: #GRC8253_166720

Course Introduction / Overview:

In today's digitally-driven landscape, the effective management of information security is no longer just an IT function but a cornerstone of corporate governance and strategic success. This course provides a comprehensive framework for establishing and maintaining a robust information security governance and risk management program. We delve into the principles articulated by thought leaders like Alan Calder in his seminal work, "IT Governance: An International Guide to Data Security and ISO27001/ISO27002," to bridge the gap between technical security controls and executive-level business objectives. Participants will explore how to align security initiatives with organizational goals, manage risks proactively, and ensure compliance with ever-evolving regulatory demands. At BIG BEN Training Center, we have designed this program to move beyond theoretical concepts, offering practical guidance on implementing frameworks such as ISO 27001 and the NIST Cybersecurity Framework. This training course empowers leaders to build a resilient security culture, make informed risk-based decisions, and demonstrate due diligence to stakeholders, ultimately transforming information security from a cost center into a strategic business enabler.

Target Audience / This training course is suitable for:

- Chief Information Security Officers (CISOs) and security directors.
- IT managers and team leaders.
- Risk managers and compliance officers.
- Internal and external auditors.
- IT governance professionals.
- Business continuity and disaster recovery planners.
- Legal and corporate governance professionals.
- Senior executives and board members with oversight of risk.

Target Sectors and Industries:

- Banking and financial services.
- Healthcare and pharmaceutical industries.
- Technology and telecommunications sectors.
- Government agencies and public sector organizations.
- Retail and e-commerce.
- Energy and utilities.
- Consulting and professional services firms.

Target Organizations Departments:

- Information Technology and Information Security.
- Risk Management and Compliance.
- Internal Audit and Assurance.
- Legal and Corporate Secretariat.
- Finance and Operations.
- Human Resources.
- Executive Management and Board of Directors.

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 strategy with business objectives and risk appetite.
- Conduct thorough risk assessments using established methodologies.
- Master the principles of the ISO 27001 and NIST Cybersecurity Frameworks.
- Design and implement effective security policies, standards, and procedures.
- Establish key performance indicators (KPIs) and metrics for security monitoring.
- Manage third-party and supply chain security risks effectively.
- Develop and lead an effective incident response and management program.
- Communicate security risks and strategies effectively to executive leadership.
- Foster a strong, security-aware culture throughout the organization.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, engaging, and practical, ensuring that participants can immediately apply their learning in a real-world context. We move beyond traditional lectures to foster a dynamic learning environment built on collaborative problem-solving and experiential activities. The course heavily incorporates case studies of real-world security breaches and successful governance implementations, allowing participants to analyze complex scenarios and debate strategic decisions. Group discussions and team-based exercises are central to our approach, encouraging the sharing of diverse perspectives and experiences. Participants will work on practical simulations, such as developing a risk treatment plan or drafting a board-level security report. Our expert instructors facilitate these sessions, providing personalized feedback and guiding participants through complex topics. This hands-on approach ensures a deep understanding of information security governance and risk management principles, equipping attendees with not just knowledge, but the confidence and skills to lead security initiatives within their own organizations.

Course Agenda (Course Units):

Unit One Foundations of Information Security Governance

- Introduction to Governance, Risk, and Compliance (GRC).
- The role of information security in corporate governance.
- Key drivers for security governance including legal and regulatory requirements.
- Distinguishing between governance and management.
- Core principles of effective information security governance.
- Establishing roles, responsibilities, and accountability structures.
- Introduction to major frameworks like COBIT and ISO 38500.

Unit Two Mastering Security Risk Management

- Principles and concepts of information risk management.
- The complete risk management lifecycle from identification to monitoring.
- Qualitative and quantitative risk assessment techniques.
- Methodologies such as FAIR (Factor Analysis of Information Risk).
- Developing a risk register and heat map.
- Defining and communicating risk appetite and tolerance.
- Strategies for risk treatment: avoidance, acceptance, mitigation, and transfer.

Unit Three Implementing Security Frameworks and Standards

- Deep dive into the ISO 27001 Information Security Management System (ISMS).
- Understanding the clauses and Annex A controls of ISO 27001.
- Practical guide to implementing the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover).
- Mapping controls between different industry standards.
- Achieving and maintaining compliance with regulations like GDPR and HIPAA.
- Developing a unified control framework for your organization.
- The role of audits in verifying framework implementation.

Unit Four Policy, Compliance, and Security Culture

- Developing a hierarchy of security policies, standards, and procedures.
- Best practices for policy lifecycle management.
- Building a robust security awareness and training program.
- Techniques for fostering a positive cybersecurity culture.
- Managing compliance with multiple regulatory bodies.
- The role of automation in compliance monitoring and reporting.
- Ethical considerations in information security.

Unit Five Strategic Leadership and Security Operations

- Managing and measuring the security program's performance.
- Developing meaningful security metrics and Key Risk Indicators (KRIs).
- Communicating security value and risk to the board of directors.
- Integrating security into the System Development Life Cycle (SDLC).
- Third-party risk management and supply chain security.
- Fundamentals of business continuity and disaster recovery planning.
- Future trends in security governance and emerging threats.

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:

In an era of rapid digital transformation, how can an organization's governance framework remain agile enough to enable innovation while being rigid enough to ensure comprehensive security and compliance?

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 corporate governance and business enablement. While many courses concentrate purely on the technical implementation of security controls or the procedural aspects of a single framework, our curriculum is designed for current and future leaders. We emphasize the development of strategic thinking, enabling participants to not only manage risk but also to articulate its business impact and advocate for security as a competitive advantage. The course uniquely bridges the communication gap between technical security teams and executive leadership, providing practical tools for creating compelling business cases and board-level reports. Rather than just teaching the "what" of standards like ISO 27001, we explore the "why" and "how," using Socratic discussion and complex case studies to foster critical decision-making skills. The program's focus on building a resilient security culture and managing third-party risk provides a holistic perspective that is essential for navigating today's interconnected and complex threat landscape.