Digital Transformation Security and Risk Governance Training Course



16 - 20 Nov 2026

Milan

5900 € (Per Person)

Ref: #CYB7539_88745

Course Introduction / Overview:

In the contemporary business landscape, digital transformation is not merely an option but a critical imperative for survival and growth. However, this rapid evolution introduces a complex web of new security vulnerabilities and risks that can undermine strategic objectives if not managed effectively. This course provides a comprehensive framework for integrating robust security and risk governance into the very fabric of digital transformation initiatives. Drawing on principles articulated by leading thinkers like Daniel J. Solove in works such as "Understanding Privacy," we explore the delicate balance between innovation and protection. This program moves beyond traditional, siloed security approaches to foster a holistic, business-aligned governance model. Participants will learn to navigate the intricate challenges of cloud adoption, IoT integration, and data analytics while ensuring regulatory compliance and building cyber resilience. At BIG BEN Training Center, we have designed this course to empower leaders to champion a culture of security, transforming it from a technical afterthought into a strategic business enabler that drives trust, value, and sustainable success in the digital age. This is a masterclass in future-proofing your organization by embedding security and risk governance at the core of your transformation journey.

Target Audience / This training course is suitable for:

- Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs).
- IT Directors and Senior IT Managers.
- Cybersecurity and Information Security Professionals.
- Risk Management and Compliance Officers.
- Internal and External Auditors.
- Project and Program Managers leading digital initiatives.
- Business Leaders and Department Heads involved in strategic planning.
- Legal and Corporate Governance Professionals.

Target Sectors and Industries:

- Banking, Financial Services, and Insurance.
- Healthcare and Pharmaceutical sectors.
- Technology, Software, and Telecommunications.
- Government Agencies and Public Sector Bodies.
- Retail, E-commerce, and Consumer Goods.
- Manufacturing and Industrial sectors (Industry 4.0).
- Energy, Utilities, and Critical Infrastructure.
- Consulting and Professional Services.

Target Organizations Departments:

- Information Technology (IT) and Operations.
- Cybersecurity and Information Security.
- Risk Management and Corporate Governance.
- Compliance and Legal Affairs.
- Internal Audit and Assurance.
- Digital Strategy and Innovation.
- Project Management Office (PMO).
- Business Operations and Development.

Course Offerings:

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

- Develop a comprehensive security governance framework tailored for digital transformation.
- Conduct advanced cybersecurity risk assessments for emerging technologies like AI and IoT.
- Align cybersecurity strategy with overarching business objectives and digital goals.
- Implement robust data governance and privacy controls in line with global regulations.
- Establish effective incident response and business continuity plans for digital services.
- Evaluate and manage third-party and supply chain security risks in a digital ecosystem.
- Communicate cybersecurity risks and strategies effectively to executive leadership and the board.
- Foster a proactive security culture throughout the organization.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and highly practical, ensuring that participants can immediately apply their learning. We move beyond theoretical lectures to a dynamic learning environment built on real-world application. The course heavily utilizes in-depth case studies of organizations that have navigated the complexities of digital transformation, analyzing both their successes and failures in security governance. Participants will engage in collaborative group workshops to design risk governance frameworks and respond to simulated cyber incidents, fostering critical thinking and teamwork. Interactive sessions, expert-led discussions, and peer-to-peer knowledge sharing are central to our approach. We emphasize a hands-on learning model where participants work on practical exercises that mirror the challenges they face in their own organizations. Continuous feedback from the instructor ensures a deep understanding of complex topics. This blended approach guarantees that attendees leave not just with knowledge, but with the confidence and skills to lead security and governance within their own digital transformation journeys.

Course Agenda (Course Units):

Unit One: Foundations of Digital Transformation and Security Governance

- The imperative of digital transformation in the modern economy.
- Understanding the expanded threat landscape and new attack vectors.
- Core principles of information security governance.
- Introduction to key governance frameworks (e.g., COBIT, NIST Cybersecurity Framework).
- Aligning security governance with business strategy and objectives.
- Defining roles and responsibilities for digital risk ownership.
- Establishing a charter for the security governance committee.

Unit Two: Strategic Cybersecurity Risk Management

- Advanced risk assessment methodologies for digital projects.
- Defining and communicating the organization's risk appetite and tolerance.
- Threat modeling for cloud, mobile, and IoT environments.
- Integrating risk management into the project lifecycle (Security by Design).
- Quantitative vs. qualitative risk analysis techniques.
- Developing and maintaining a comprehensive risk register.
- Techniques for effective risk treatment and mitigation.

Unit Three: Securing the Digital Ecosystem and Emerging Technologies

- Cloud security governance and shared responsibility models.
- Securing Internet of Things (IoT) and Operational Technology (OT) systems.
- Implementing DevSecOps principles for secure software development.
- Architecting for security with a Zero Trust model.
- Advanced Identity and Access Management (IAM) strategies.
- Data Loss Prevention (DLP) technologies and implementation.
- Security considerations for Artificial Intelligence (AI) and Machine Learning (ML).

Unit Four: Data Governance, Privacy, and Regulatory Compliance

- Principles of effective data governance in a digital age.
- Navigating global privacy regulations (GDPR, CCPA, etc.).
- Implementing Privacy by Design and by Default.
- Strategies for data classification, protection, and lifecycle management.
- Managing cross-border data transfer complexities.
- Developing a robust data breach and incident notification plan.
- Ensuring compliance in third-party and vendor relationships.

Unit Five: Leadership, Resilience, and Future-Proofing Governance

- Communicating risk and security strategy to the Board of Directors.
- Developing and reporting meaningful cybersecurity metrics and KPIs.
- Building a resilient organization through effective business continuity planning.
- Leading and managing a high-performing cybersecurity team.
- Cultivating a strong, organization-wide security awareness culture.
- Preparing for future threats and technological shifts.
- Crisis management and leadership during a major cyber incident.

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 AI and machine learning become more integrated into core business processes, how must traditional risk governance frameworks evolve to address the unique, opaque, and autonomous nature of AI-driven threats?

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

This course distinguishes itself by adopting a strategic, top-down perspective on cybersecurity, treating it not as a technical function but as a core pillar of business governance in the digital era. While other courses may focus narrowly on specific technologies or compliance checklists, our curriculum is uniquely designed to bridge the critical gap between technical security teams, risk management functions, and executive leadership. We provide a holistic risk perspective that integrates cybersecurity into the entire lifecycle of digital transformation, from initial strategy to ongoing operations. The program emphasizes the development of leadership and communication skills, empowering participants to articulate complex security risks in clear business terms to a board-level audience. Furthermore, the content is forward-looking, moving beyond current best practices to explore the governance challenges of emerging technologies like AI and quantum computing. By focusing on actionable frameworks, strategic alignment, and building a culture of cyber resilience, this course equips leaders with the comprehensive capabilities needed to govern risk and enable secure innovation, rather than just managing technical controls.