Cybersecurity Governance for Digital Transformation Leaders Training Course



19 - 23 Oct 2026

Milan

5900 € (Per Person)

Ref: #DT1296_92524

Course Introduction / Overview:

In an era where digital transformation is not just an option but a necessity for survival and growth, the alignment of cybersecurity with business strategy is paramount. This course addresses the critical intersection of cybersecurity governance and digital transformation, providing leaders with the strategic foresight to navigate complex digital risks. It moves beyond traditional, reactive security measures to a proactive governance model that enables innovation while safeguarding critical assets. Drawing on principles discussed by thought leaders like Peter Weill and Stephanie L. Woerner in works such as "What's Your Digital Business Model?", the curriculum emphasizes how robust governance is a key enabler of digital agility and resilience. Participants will learn to build and lead a security-conscious culture, ensuring that cybersecurity is integrated into the fabric of every digital initiative. At BIG BEN Training Center, we have designed this program to equip leaders with the tools to make informed decisions, manage third-party risks, and communicate effectively with stakeholders, transforming cybersecurity from a cost center into a strategic business advantage.

Target Audience / This training course is suitable for:

- Chief Information Officers (CIOs) and Chief Technology Officers (CTOs).
- Chief Information Security Officers (CISOs) and IT Security Directors.
- Digital Transformation Program Managers and Leaders.
- Senior Business Executives and Board Members.
- IT Governance, Risk, and Compliance (GRC) Professionals.
- Enterprise Architects and Senior IT Managers.
- Heads of Legal, Audit, and Corporate Strategy.

Target Sectors and Industries:

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

Target Organizations Departments:

- Executive Management and Leadership.
- Information Technology and Information Security.
- Digital Strategy and Innovation.
- Risk Management and Compliance.
- Internal Audit and Assurance.
- Legal and Corporate Governance.
- Strategic Planning and Business Development.

Course Offerings:

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

- Develop a comprehensive cybersecurity governance framework tailored for digital transformation.
- Align cybersecurity strategy with overarching business objectives and innovation goals.
- Implement robust risk management processes for emerging technologies like cloud, AI, and IoT.
- Lead the cultivation of a proactive and pervasive cybersecurity culture across the organization.
- Master the art of communicating cyber risks and strategies to the board and executive leadership.
- Navigate the complex landscape of global data privacy and cybersecurity regulations.
- Design and oversee effective incident response and business continuity plans.
- Evaluate and manage cybersecurity risks associated with third-party vendors and partners.
- Establish meaningful metrics to measure the effectiveness of the cybersecurity program.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and directly applicable to the participant's professional environment. This course eschews traditional lecture-based formats in favor of a dynamic learning experience. We utilize a blend of expert-led presentations, in-depth case study analyses of real-world digital transformation successes and failures, and facilitated group discussions that encourage peer-to-peer learning. Participants will engage in practical workshops and simulation exercises to apply governance concepts to realistic business scenarios, such as developing a board-level report on cyber risk or creating a governance policy for a new AI implementation. Emphasis is placed on strategic thinking and problem-solving, with continuous feedback from the instructor and peers. This hands-on approach ensures that leaders not only understand the theoretical frameworks of cybersecurity governance but also develop the practical skills and confidence to implement them effectively within their own organizations, driving secure and successful digital transformation.

Course Agenda (Course Units):

Unit One: Foundations of Governance in the Digital Age

- Defining Digital Transformation and its security implications.
- The core principles of modern cybersecurity governance.
- Distinguishing between governance, management, and operations.
- The strategic role of the CISO and other executive leaders.
- Aligning security initiatives with business strategy and value creation.
- Understanding the threat landscape in a hyper-connected environment.
- Case study on governance failures in major digital projects.

Unit Two: Strategic Frameworks and Integrated Risk Management

- Exploring key governance frameworks (NIST CSF, COBIT, ISO 27001).
- Developing a tailored governance framework for your organization.
- Conducting a comprehensive digital risk assessment.
- Quantitative vs. qualitative risk analysis techniques.
- Building a risk register and defining risk appetite.
- Integrating cybersecurity risk into enterprise risk management (ERM).
- Third-party and supply chain risk management strategies.

Unit Three: Governing Emerging Technologies

- Cloud security governance models (IaaS, PaaS, SaaS).
- Data governance and privacy in the cloud.
- Securing the Internet of Things (IoT) and operational technology (OT).
- Governance challenges of Artificial Intelligence (AI) and Machine Learning (ML).
- Developing policies for secure software development (DevSecOps).
- Implementing a Zero Trust architecture approach.
- Ethical considerations in data usage and digital innovation.

Unit Four: Leadership, Culture, and Regulatory Compliance

- Cultivating a security-first organizational culture.
- The leader's role in championing cybersecurity.
- Effective communication of cyber risk to the board of directors.
- Developing and implementing security awareness and training programs.
- Navigating the global regulatory landscape (GDPR, CCPA, etc.).
- Managing legal and compliance obligations during a breach.
- Building effective cross-functional security committees.

Unit Five: Cyber Resilience and Future-Proofing Governance

- Developing a robust incident response and crisis management plan.
- Business continuity and disaster recovery planning for digital services.
- Conducting effective post-incident reviews and learning from failures.
- Establishing key performance indicators (KPIs) and metrics for governance.
- The role of cybersecurity audits and continuous monitoring.
- Anticipating future trends in technology and cyber threats.
- Creating an agile and adaptive governance model for sustained success.

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 becomes more integrated into core business processes, how must traditional cybersecurity governance models evolve to address autonomous decision-making and algorithmic bias?

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

This course distinguishes itself by focusing on the strategic synthesis of cybersecurity, leadership, and business innovation, rather than solely on technical controls or compliance checklists. While other programs may teach the "what" of security frameworks, we concentrate on the "how" and "why" for executive leaders driving digital change. The curriculum is uniquely designed to bridge the communication gap between technical security teams and the C-suite, empowering participants to articulate cyber risk in the language of business value, opportunity, and strategic advantage. We move beyond fear-based security narratives to a model of security as a business enabler. The course content is enriched with forward-looking modules on governing emerging technologies like AI and IoT, ensuring leaders are prepared not just for today's challenges but for the digital ecosystem of tomorrow. The emphasis on case studies, strategic simulations, and peer-led discussions provides a level of practical, decision-making insight that is rare in the training landscape, making it an essential program for any leader at the helm of digital transformation.