Integrated Data Privacy and Cybersecurity Risk Training Course

14 - 18 Dec 2026

Milan

5900 € (Per Person)

Ref: #DM5665_90582

Course Introduction / Overview:

In today's digitally-driven landscape, the distinction between data privacy and cybersecurity has blurred, creating a complex and critical risk environment for all organizations. This course provides a comprehensive, integrated approach to managing these intertwined challenges. It moves beyond treating privacy and security as separate functions, instead presenting a unified strategy for protecting sensitive information and mitigating cyber threats. As articulated by the renowned privacy scholar Daniel J. Solove in his works like "Understanding Privacy," true data protection requires a synthesis of legal compliance and robust technical security. This program, offered by BIG BEN Training Center, is meticulously designed to equip professionals with the knowledge and skills to build and maintain resilient data protection programs. We will explore everything from foundational principles and global regulations like GDPR and CCPA to advanced topics such as threat modeling, incident response, and third-party risk management. Participants will gain a holistic understanding of how to conduct data protection impact assessments, implement privacy by design, and align security controls with privacy obligations, ensuring their organization not only complies with the law but also builds trust with its stakeholders in an era of increasing digital scrutiny.

Target Audience / This training course is suitable for:

- Information Security Managers and Analysts.
- IT Managers and System Administrators.
- Data Protection Officers (DPOs) and Privacy Professionals.
- Compliance Officers and Managers.
- Legal Counsel and Corporate Lawyers.
- Risk Management Professionals and Analysts.
- Internal and External Auditors.
- Project Managers handling sensitive data.
- Human Resources Managers.
- Senior executives with oversight of risk and compliance.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Technology and Telecommunications.
- Retail and E-commerce.
- Governmental agencies and public sector bodies.
- Consulting and Professional Services.
- Education and Research Institutions.
- Energy and Utilities.

Target Organizations Departments:

- Information Technology (IT) and Information Security.
- Legal and Compliance.
- Risk Management.
- Internal Audit.
- Human Resources.
- Procurement and Vendor Management.
- Operations.
- Marketing and Sales.
- Research and Development.

Course Offerings:

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

- Develop a comprehensive data privacy governance framework.
- Conduct thorough cybersecurity risk assessments using industry-standard methodologies.
- Interpret and apply key requirements of major data privacy regulations like GDPR and CCPA.
- Implement Privacy by Design and by Default principles in projects and systems.
- Formulate and test an effective data breach and incident response plan.
- Evaluate and manage third-party vendor and supply chain security risks.
- Align information security controls with data privacy principles.
- Perform Data Protection Impact Assessments (DPIAs) for high-risk processing activities.
- Foster a culture of security and privacy awareness throughout the organization.
- Navigate the complexities of cross-border data transfers and their legal implications.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and highly practical. We believe that adult learning is most effective when it combines theoretical knowledge with hands-on application. This course utilizes a blended approach, featuring expert-led presentations, in-depth case study analyses of real-world data breaches and privacy failures, and dynamic group discussions that encourage peer-to-peer learning. Participants will engage in practical workshops and simulation exercises, such as conducting a mock risk assessment or drafting a preliminary incident response plan. These interactive sessions are designed to bridge the gap between theory and practice, allowing attendees to apply concepts to tangible business scenarios. Our instructors facilitate a collaborative environment, providing continuous feedback and encouraging participants to share their unique organizational challenges. The curriculum is structured to build knowledge progressively, ensuring that complex topics are accessible and that participants leave with not just information, but with actionable strategies and a robust toolkit they can implement immediately within their roles.

Course Agenda (Course Units):

Unit One: Foundations of Data Privacy and Cybersecurity

- The Intersection of Privacy and Security.
- Key Terminology and Concepts in Data Protection.
- Historical Evolution of Privacy Rights and Cyber Threats.
- Introduction to Global Privacy Laws (GDPR, CCPA, LGPD).
- Core Principles of Information Security (Confidentiality, Integrity, Availability).
- Understanding the Threat Landscape and Attack Vectors.
- The Role of Ethics in Data Handling and Security.

Unit Two: Risk Management and Governance Frameworks

- Introduction to Cybersecurity Risk Management.
- Implementing the NIST Cybersecurity Framework (CSF).
- Conducting a Comprehensive Risk Assessment.
- Information Security Governance and Policy Development.
- Introduction to ISO/IEC 27001 and 27701 Standards.
- Threat Modeling and Vulnerability Management.
- Developing a Risk Treatment and Mitigation Plan.

Unit Three: Implementing a Data Privacy Program

- The Role of the Data Protection Officer (DPO).
- Building a Data Inventory and Mapping Data Flows.
- Conducting Data Protection Impact Assessments (DPIAs).
- Principles of Privacy by Design and by Default.
- Managing Data Subject Rights (Access, Rectification, Erasure).
- Legal Bases for Processing Personal Data and Consent Management.
- Policies for Data Retention and Secure Disposal.

Unit Four: Cybersecurity Controls and Incident Response

- Technical Security Controls (Encryption, Access Control, Network Security).
- Administrative and Physical Security Controls.
- Developing a Security Awareness and Training Program.
- Creating a Data Breach and Incident Response Plan.
- Incident Detection, Triage, and Analysis.
- Containment, Eradication, and Recovery Strategies.
- Post-Incident Analysis and Regulatory Notification Requirements.

Unit Five: Advanced Topics and Future-Proofing

- Managing Third-Party and Vendor Security Risk.
- Cloud Security and Data Privacy in the Cloud.
- Securing IoT and Operational Technology (OT) Environments.
- Privacy Enhancing Technologies (PETs).
- Navigating Cross-Border Data Transfer Mechanisms.
- Preparing for Audits and Demonstrating Compliance.
- Emerging Threats and the Future of Privacy and Cybersecurity.

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 data becomes the new currency, how can organizations ethically balance data monetization with the fundamental right to individual privacy?

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

This course distinguishes itself by its holistic and integrated approach, treating data privacy and cybersecurity not as separate silos but as two sides of the same coin. While many programs focus heavily on either the legal-compliance aspects of privacy or the technical mechanics of security, our curriculum is meticulously designed to synthesize these domains. We provide a strategic management perspective, empowering participants to build comprehensive data protection programs that are both legally sound and technically robust. The emphasis is on practical application and strategic thinking rather than just tool-specific training. Participants will learn to conduct risk assessments that account for privacy harms, implement security controls that directly support data protection principles, and develop incident response plans that address both operational recovery and regulatory notification obligations. The content moves beyond mere compliance checklists to foster a deep understanding of the principles behind the regulations, enabling professionals to make informed, risk-based decisions and future-proof their organizations against an evolving landscape of threats and legal requirements.