Integrated Records Management and Information Security Training Course



07 - 11 Dec 2026

Milan

5900 € (Per Person)

Ref: #SA1359_25782

Course Introduction / Overview:

In today's data-driven world, the convergence of records management and information security is no longer optional, it is a critical business imperative. This training course provides a comprehensive framework for professionals seeking to master the integrated governance of information assets. We will move beyond traditional, siloed approaches to explore how a unified strategy can protect sensitive data, ensure regulatory compliance, and enhance organizational efficiency. Drawing on foundational principles outlined by experts like Jason R. Baron and in seminal works such as "Records and Information Management" by Patricia C. Franks, this program delves into the complete records lifecycle, from creation to secure disposal. Participants will learn to navigate the complex landscape of data privacy regulations, implement robust security controls, and build a resilient information governance framework. BIG BEN Training Center has designed this course to equip attendees with the practical skills needed to manage both digital and physical records securely, mitigate risks, and lead their organizations through the challenges of digital transformation with confidence and strategic foresight.

Target Audience / This training course is suitable for:

- Records Managers and Information Management Professionals.
- IT Security Specialists and Cybersecurity Analysts.
- Compliance Officers and Risk Managers.
- Data Protection Officers (DPOs) and Privacy Professionals.
- Legal Counsel and Paralegals.
- Archivists and Librarians.
- Operations Managers and Department Heads.
- Internal and External Auditors.
- Senior Administrators responsible for information governance.

Target Sectors and Industries:

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

Target Organizations Departments:

- Information Technology (IT) and Cybersecurity.
- Legal and Compliance.
- Risk Management.
- Records and Information Management (RIM).
- Internal Audit.
- Operations and Administration.
- Human Resources (HR).
- Finance and Accounting.
- Corporate Governance.

Course Offerings:

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

- Develop and implement a comprehensive information governance framework.
- Master the principles of the records lifecycle from creation to disposition.
- Design and manage effective records retention and disposal schedules.
- Implement information security controls based on the ISO 27001 standard.
- Conduct information risk assessments and develop mitigation strategies.
- Ensure compliance with major data privacy regulations like GDPR and CCPA.
- Classify data and information assets according to sensitivity and business value.
- Develop and execute a data breach incident response plan.
- Manage e-discovery requests and legal holds effectively.
- Audit and monitor the effectiveness of records management and security programs.
- Leverage technology for secure digital records management and archiving.

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. Our approach moves beyond traditional lectures to foster a dynamic learning environment. The course will feature a blend of expert-led presentations, in-depth case study analyses of real-world data breaches and compliance failures, and interactive group discussions that encourage peer-to-peer learning. Participants will engage in hands-on workshops to practice skills such as conducting risk assessments and developing information security policies. Team-based exercises will simulate incident response scenarios, challenging participants to collaborate and make critical decisions under pressure. Throughout the course, there will be continuous opportunities for Q&A sessions and direct feedback from the instructor. This immersive and participatory methodology ensures a deep understanding of both the strategic principles and the tactical application of integrated records management and information security governance.

Course Agenda (Course Units):

Unit One: Foundations of Information Governance

- Introduction to Records Management and Information Security.
- The Strategic Importance of an Integrated Governance Framework.
- Key Concepts: Records, Information, Data, and Assets.
- International Standards: ISO 15489 for Records Management.
- The Legal and Regulatory Environment for Information.
- Roles and Responsibilities in Information Governance.
- Developing a Business Case for an Integrated Program.

Unit Two: Mastering the Records Management Lifecycle

- Phase 1: Record Creation, Capture, and Control.
- Phase 2: Classification, Indexing, and Metadata Management.
- Phase 3: Secure Storage, Access, and Use Policies.
- Phase 4: Developing and Implementing Retention Schedules.
- Phase 5: Secure Disposition, Destruction, and Archiving.
- Managing Physical vs. Digital Records.
- Special Considerations for Email and Social Media Records.

Unit Three: Principles of Information Security Management

- The CIA Triad: Confidentiality, Integrity, and Availability.
- Introduction to ISO 27001 and the Information Security Management System (ISMS).
- Conducting an Information Security Risk Assessment.
- Implementing Core Security Controls: Access Control, Encryption, and Network Security.
- Developing Information Security Policies and Procedures.
- Security Awareness and Training Programs for Employees.
- Physical and Environmental Security for Information Assets.

Unit Four: Integrating Security, Privacy, and Compliance

- Building an Integrated Information Governance Framework.
- Aligning Records Management with Security and Privacy Policies.
- Navigating Global Data Privacy Regulations (GDPR, CCPA).
- Data Classification Schemes and Secure Handling Procedures.
- Incident Response Planning and Data Breach Management.
- Business Continuity and Disaster Recovery for Records.
- Third-Party Risk Management and Vendor Due Diligence.

Unit Five: Advanced Topics and Future-Proofing Your Program

- Electronic Discovery (E-Discovery) and Legal Hold Processes.
- Managing Records in the Cloud and Hybrid Environments.
- Auditing and Monitoring Your Information Governance Program.
- Metrics and Reporting for Program Effectiveness.
- Emerging Technologies: AI, Blockchain, and Automation in Records Management.
- Ethical Considerations in Information Handling.
- Creating a Culture of Information Governance and Security.

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 AI adoption, how can organizations balance the utility of large language models with the fundamental principles of records integrity and information security?

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

This course distinguishes itself by its holistic and integrated approach, treating records management and information security not as separate disciplines but as two essential pillars of a single, unified information governance strategy. While many courses focus on one area or the other, we provide a comprehensive curriculum that bridges the gap, equipping participants with the versatile skills needed to manage the modern information landscape. The program is built on a foundation of internationally recognized standards, such as ISO 15489 and ISO 27001, focusing on practical implementation rather than just theoretical knowledge. We emphasize the real-world application of concepts through extensive use of case studies, interactive simulations of data breach scenarios, and hands-on policy development workshops. Furthermore, the course is forward-looking, addressing the complex challenges posed by emerging technologies like cloud computing and artificial intelligence, and navigating the intricate web of global data privacy regulations. This strategic, practical, and future-focused perspective ensures participants leave not just with knowledge, but with the actionable expertise to build resilient and compliant information governance programs within their organizations.