Strategic Information Governance and Data Privacy Training Course

Ref: #GRC2754

Course Introduction / Overview:

In today's data-driven economy, information is the most critical asset for any organization, yet it also presents significant risks. This course provides a comprehensive framework for managing these challenges effectively. The curriculum is designed to bridge the gap between legal compliance, IT security, and business strategy, establishing a holistic approach to data management. We delve into the principles articulated by global thought leaders like Ann Cavoukian, the creator of the 'Privacy by Design' framework, ensuring that privacy is proactively embedded into all organizational processes. This program moves beyond theoretical knowledge, focusing on the practical implementation of robust information governance and data privacy programs. Participants will learn to navigate the complex landscape of regulations such as GDPR and CCPA, transforming compliance obligations into a competitive advantage. At BIG BEN Training Center, we empower professionals to build a culture of data responsibility, safeguard sensitive information, and unlock the true value of their data assets securely and ethically, a theme well-explored in texts like "Information Governance: Concepts, Strategies, and Best Practices" by Robert F. Smallwood. This course is the definitive guide for professionals seeking to lead their organizations in an era of digital transformation and heightened regulatory scrutiny.

Target Audience / This training course is suitable for:

- Data Protection Officers (DPOs).
- Compliance and Privacy Professionals.
- IT Managers and Information Security Analysts.
- Legal Counsel and Corporate Lawyers.
- Risk Management Specialists.
- Records Managers and Archivists.
- Senior Business Leaders and Executives.
- Human Resources Managers.
- Internal and External Auditors.
- Project Managers handling sensitive data.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Technology and Telecommunications.
- Retail and E-commerce.
- Governmental and Public Sector Agencies.
- Consulting and Professional Services.
- Education and Research Institutions.
- Insurance and Risk Management.

Target Organizations Departments:

- Legal and Compliance Departments.
- Information Technology (IT) and Information Security.
- Risk Management and Internal Audit.
- Human Resources (HR).
- Marketing and Sales.
- Operations and Administration.
- Finance and Accounting.
- Customer Service and Support.

Course Offerings:

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

- Develop and implement a comprehensive information governance framework.
- Navigate the legal and regulatory requirements of major data protection laws like GDPR and CCPA.
- Conduct Data Protection Impact Assessments (DPIAs) to identify and mitigate privacy risks.
- Master the principles of Privacy by Design and Privacy by Default.
- Establish effective data classification, retention, and disposal policies.
- Formulate and manage a robust data breach incident response plan.
- Define roles and responsibilities for data stewardship and ownership across the organization.
- Audit and monitor the effectiveness of data privacy controls and procedures.
- Address the challenges of cross-border data transfers and third-party vendor risk.
- Foster a culture of data privacy awareness and accountability within the organization.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and highly practical. We believe that effective learning in the fields of data privacy and information governance comes from applying concepts to real-world scenarios. The course structure emphasizes a blend of expert-led instruction, collaborative group discussions, and hands-on exercises. Participants will engage with detailed case studies drawn from various industries, analyzing both successful governance implementations and notable data breach incidents to extract critical lessons. Interactive workshops will guide attendees through the process of creating key documentation, such as data maps, privacy policies, and incident response playbooks. Team-based activities encourage peer-to-peer learning and the sharing of diverse professional experiences, creating a rich and dynamic learning environment. Our expert instructors facilitate sessions that are not just lectures but guided conversations, ensuring that every participant has the opportunity to ask questions, challenge assumptions, and receive personalized feedback. This experiential approach ensures that attendees leave not only with theoretical knowledge but also with the confidence and practical skills to implement effective data governance and privacy strategies immediately within their own organizations.

Course Agenda (Course Units):

Unit One: Foundations of Data Privacy and Information Governance

- Introduction to Information Governance (IG).
- The core principles of data privacy.
- Distinguishing between data privacy, data protection, and information security.
- Global legal and regulatory landscapes (GDPR, CCPA, etc.).
- The role of the Data Protection Officer (DPO) and other key stakeholders.
- Understanding personal data and sensitive personal information.
- The ethical considerations of data handling and processing.
- The business case for robust information governance.

Unit Two: Developing an Information Governance Framework

- Establishing an IG steering committee and defining roles.
- Creating and implementing IG policies and procedures.
- Data classification schemes and handling standards.
- Developing a comprehensive data map and record of processing activities (ROPA).
- Information lifecycle management from creation to disposal.
- Records and information management (RIM) principles.
- Setting up a data retention and disposition schedule.
- Communicating the IG framework across the organization.

Unit Three: Operationalizing Data Privacy Management

- The seven principles of Privacy by Design (PbD).
- Conducting Data Protection Impact Assessments (DPIAs).
- Managing data subject rights (access, rectification, erasure).
- Mechanisms for lawful data processing and consent management.
- Privacy considerations in marketing and digital analytics.
- Implementing privacy-enhancing technologies (PETs).
- Vendor and third-party risk management strategies.
- Training and awareness programs for employees.

Unit Four: Information Security and Incident Response

- Integrating information security controls within the IG framework.
- Key security concepts: confidentiality, integrity, and availability.
- Common cyber threats and vulnerabilities.
- Developing a data breach incident response plan.
- Steps for containment, investigation, and eradication of threats.
- Notification requirements for regulators and affected individuals.
- Post-incident analysis and continuous improvement.
- Business continuity and disaster recovery planning for data.

Unit Five: Auditing, Monitoring, and Future Trends

- Developing metrics and KPIs to measure IG program effectiveness.
- Techniques for auditing and monitoring compliance.
- Managing cross-border data transfers and adequacy mechanisms.
- The impact of emerging technologies like AI and IoT on data privacy.
- Data ethics and responsible innovation.
- Preparing for regulatory investigations and enforcement actions.
- The future of data protection and information governance.
- Final project: Developing a strategic IG roadmap.

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 advancing AI and big data analytics, how can organizations balance the drive for data-driven innovation with the fundamental ethical obligation to protect individual privacy?

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

This course distinguishes itself by adopting a strategic, business-integrated perspective on data privacy and information governance, rather than a purely compliance-driven or technical viewpoint. While many programs focus narrowly on the legal requirements of regulations like GDPR, our curriculum emphasizes how to build a comprehensive governance framework that not only ensures compliance but also enhances business value, mitigates risk, and builds customer trust. We move beyond the "what" and "why" to focus intensely on the "how," providing participants with actionable methodologies, templates, and practical skills. The course uniquely integrates the three pillars of privacy, security, and records management into a single, cohesive strategy, addressing the operational silos that often undermine data protection efforts. Our emphasis on Privacy by Design, data ethics, and fostering a corporate culture of data responsibility prepares professionals not just for today's challenges but for the future landscape of emerging technologies. The content is designed to empower leaders to have strategic conversations with C-suite executives, translating complex legal and technical requirements into clear business imperatives and competitive differentiators.