Information Security Manager (CISM) Prep Training Course

14 - 18 Dec 2026

Rome

5800 € (Per Person)

Ref: #CYB6246_89076

Course Introduction / Overview:

This course provides a comprehensive and accelerated path for professionals aiming to achieve the globally recognized Certified Information Security Manager (CISM) designation. It is meticulously designed to cover the four core domains of the CISM body of knowledge, moving beyond purely technical skills to focus on the strategic management of an enterprise's information security. In today's digital landscape, the role of an information security manager is pivotal in aligning security programs with business goals and managing organizational risk effectively. This program delves into the principles articulated by leading academics like Michael E. Whitman and Herbert J. Mattord in their seminal work, "Management of Information Security". Participants will explore how to establish and maintain an information security governance framework, manage complex information risks, and develop and oversee a robust security program. BIG BEN Training Center has structured this course to not only prepare candidates for the CISM exam but also to equip them with the practical, real-world competencies required to lead security initiatives, make informed decisions, and communicate security's value to executive leadership, thereby becoming an indispensable asset to their organization.

Target Audience / This training course is suitable for:

- Aspiring Certified Information Security Managers.
- IT Managers and Directors.
- Information Security Professionals.
- IT Auditors and Consultants.
- Risk Management Professionals.
- Compliance Officers.
- Network and Security Administrators with management goals.
- Executives with information security responsibilities.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Information Technology and Telecommunications.
- Governmental and Public Sector Agencies.
- Consulting and Professional Services.
- Energy and Utilities.
- Retail and E-commerce.
- Manufacturing and Engineering.

Target Organizations Departments:

- Information Technology and Information Security.
- Internal Audit and Assurance.
- Risk Management and Compliance.
- Legal and Corporate Governance.
- Operations Management.
- Strategic Planning and Business Development.
- Human Resources.
- Finance and Administration.

Course Offerings:

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

- Develop and maintain an information security governance framework to align with business strategy.
- Establish and manage an effective information risk management program.
- Design, implement, and manage a comprehensive information security program.
- Define processes for security operations and administration.
- Master the principles of information security incident management and response.
- Integrate security requirements into organizational processes and lifecycle management.
- Develop and deliver effective security awareness and training programs.
- Measure, monitor, and report on the effectiveness of security controls and metrics.
- Prepare strategically for the CISM certification exam.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, engaging, and directly applicable to the professional challenges faced by participants. This course moves beyond traditional lecture-based learning by integrating a blended approach that includes expert-led instruction, collaborative group discussions, and intensive case study analysis. We believe that adult learning is most effective when it is experiential. Therefore, participants will engage in practical exercises and simulations that mirror real-world security management scenarios, allowing them to apply theoretical concepts to tangible problems. The curriculum emphasizes peer-to-peer learning, where professionals from diverse backgrounds can share insights and best practices. Our instructors act as facilitators, guiding discussions and providing personalized feedback to ensure a deep understanding of the CISM domains. The course structure encourages critical thinking and strategic problem-solving, ensuring that participants not only absorb the material required for the exam but also develop the leadership and management acumen expected of a top-tier Information Security Manager.

Course Agenda (Course Units):

Unit One: Information Security Governance

- Fundamentals of Corporate Governance and Security Governance.
- Developing an Information Security Strategy Aligned with Business Goals.
- The Role of the Information Security Manager.
- Establishing a Governance Framework and Organizational Structure.
- Legal, Regulatory, and Contractual Requirements.
- Defining and Implementing Security Policies, Standards, and Procedures.
- Strategic Planning and Resource Management for Security.

Unit Two: Information Risk Management

- The Principles of Information Risk Management.
- Identifying and Classifying Information Assets.
- Conducting Threat and Vulnerability Assessments.
- Implementing a Risk Assessment and Analysis Methodology.
- Risk Mitigation, Transfer, Acceptance, and Avoidance Strategies.
- Integrating Risk Management into the System Development Life Cycle (SDLC).
- Monitoring and Reporting on Risk and Control Effectiveness.

Unit Three: Information Security Program Development

- Building an Information Security Program Roadmap.
- Designing Security Architecture and Infrastructure.
- Implementing Security Controls and Countermeasures.
- Data Classification and Ownership Principles.
- Identity and Access Management Solutions.
- Security Awareness, Training, and Education Programs.
- Managing Third-Party and Vendor Security Risk.

Unit Four: Information Security Program Management

- Managing Security Operations and Services.
- Developing and Monitoring Security Metrics (KPIs and KAIs).
- Business Impact Analysis (BIA) and its Role in Security.
- Business Continuity and Disaster Recovery Planning.
- Change and Configuration Management for Security.
- Vulnerability Management and Security Testing.
- Ensuring Ongoing Compliance with Policies and Standards.

Unit Five: Information Security Incident Management and Exam Preparation

- Developing an Incident Management and Response Plan.
- Establishing and Training an Incident Response Team (IRT).
- Incident Detection, Triage, and Analysis Techniques.
- Containment, Eradication, and Recovery Processes.
- Post-Incident Activities and Forensic Investigation Principles.
- Communication Strategies During and After an Incident.
- Comprehensive CISM Exam Review and Test-Taking Strategies.

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 increasingly sophisticated state-sponsored cyber-attacks, how can an Information Security Manager balance the need for robust, expensive security controls with the organization's finite budget and risk appetite?

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

This course distinguishes itself by focusing on the strategic, business-centric mindset required of a modern Information Security Manager, rather than being a purely technical or exam-cramming session. While comprehensive exam preparation is a core component, our curriculum is built around the philosophy that a CISM professional is a business leader first and a technologist second. We emphasize the development of critical thinking and decision-making skills through the extensive use of real-world case studies that challenge participants to solve complex governance, risk, and incident management problems. The course delves into the nuances of communicating risk in business terms to executive boards and stakeholders, a crucial skill often overlooked in other programs. Furthermore, the interactive methodology fosters a rich learning environment where participants learn not only from the expert instructor but also from the diverse experiences of their peers across various industries. This approach ensures that graduates leave not just with the knowledge to pass an exam, but with the strategic wisdom and practical confidence to lead and transform an enterprise's information security posture.