GAQM®
Global Association for Quality Management

Certified Information Systems Security Manager (CISSM)®

Course Outline

www.gaqm.org

CISSM Certification Overview

The Certified Information Systems Security Manager (CISSM) certification is designed for professionals responsible for establishing, managing, and governing enterprise-wide information security programs. It focuses on aligning security initiatives with business objectives, ensuring effective risk management, and implementing robust governance frameworks. CISSM emphasizes a managerial and strategic perspective, enabling candidates to design security policies, oversee security operations, and ensure compliance with legal, regulatory, and industry standards.

CISSM is ideal for security managers, IT managers, risk and compliance professionals, and aspiring security leaders who are involved in decision-making and oversight of information security functions. The certification equips professionals with the knowledge to manage security teams, evaluate emerging threats, and communicate security posture effectively to senior management and stakeholders.
By earning CISSM, professionals demonstrate their capability to lead and sustain resilient information security programs in today's evolving digital landscape.

Target Audience

The Certified Information Systems Security Manager (CISSM) certification is aimed at professionals who are responsible for managing, leading, and overseeing information security programs within an organization. This includes Information Security Managers, IT Managers, Risk and Compliance Officers, Security Consultants, and Chief Information Security Officers (CISOs).

It is also suitable for professionals aspiring to take on managerial or leadership roles in information security, who need a strategic understanding of security governance, risk management, and compliance, along with the ability to align security initiatives with business objectives. Essentially, CISSM targets anyone involved in planning, implementing, and maintaining enterprise-wide security programs.

Module Information

Module 1 - Information Security Governance

Principles of information security governance
Alignment of security strategy with business objectives
Roles and responsibilities of security management
Security policies, standards, and procedures
Legal, regulatory, and compliance requirements

Module 2 - Risk Management

Risk management frameworks and methodologies
Risk identification, assessment, and analysis
Qualitative vs quantitative risk analysis
Risk treatment options (mitigate, transfer, accept, avoid)
Risk appetite and tolerance

Module 3 - Information Security Program Development

Building an information security program
Security program lifecycle
Budgeting and resource planning
Metrics and key performance indicators (KPIs)
Continuous improvement of security programs

Module 4 - Asset Management and Data Classification

Information asset identification
Data classification models
Data ownership and custodianship
Information lifecycle management
Data handling and retention requirements

Module 5 - Security Architecture and Controls

Security architecture concepts
Defense-in-depth strategy
Administrative, technical, and physical controls
Network, application, and endpoint security
Cloud and virtualization security fundamentals

Module 6 - Identity and Access Management (IAM)

Authentication and authorization models
Role-based and attribute-based access control
Privileged access management (PAM)
Identity lifecycle management
Single sign-on (SSO) and federation

Module 7 - Security Operations and Incident Management

Security monitoring and logging
Incident response lifecycle
Threat detection and analysis
Digital forensics fundamentals
Security operations center (SOC) function

Module 8 - Business Continuity and Disaster Recovery

Business impact analysis (BIA)
Business continuity planning (BCP)
Disaster recovery strategies
Backup and recovery mechanisms
Crisis management and communication

Module 9 - Vendor, Third-Party, and Cloud Risk Management

Third-party risk assessment
Contractual and SLA security requirements
Cloud shared responsibility model
Supply chain security risks
Ongoing vendor monitoring

Module 10 - Security Compliance, Audit, and Assurance

Security audits and assessments
Compliance frameworks (ISO 27001, NIST, etc.)
Internal and external audit coordination
Security reporting to management
Continuous compliance monitoring