CISM: CERTIFIED INFORMATION SECURITY MANAGER

Course Introduction:

The **Certified Information Security Manager (CISM)** is a top credential for IT professionals responsible for managing, developing and overseeing information security systems in enterprise-level applications, or for developing best organizational security practices. The **Information Systems Audit and Control Association (ISACA)** introduced the **CISM** credential to security professionals in 2003.

ISACA's organizational goals are specifically geared toward IT professionals interested in the highest quality standards with respect to audit, control and security of information systems. The **CISM** credential targets the needs of IT security professionals with enterprise-level security management responsibilities. Credential holders possess advanced and proven skills in security risk management, program development and management, governance, and incident management and response.

The **CISM Certification** program was developed by ISACA for experienced information security management professionals who have experience developing and managing information security programs and who understand the programs relationship to the overall business goals. The **CISM Exam** consists of 200 multiple-choice questions that cover the four **CISM** domains. The American National Standards Institute (ANSI) has accredited the **CISM Certification** program under ISO/IEC 17024:2003, General Requirements for Bodies Operating Certification Systems of Persons.

What You'll Learn:

IT professionals must have 5 years or more of IS audit, control, assurance and security experience.

- Information Security Governance
- Information Risk Management and Compliance
- Information Security Program Development and Management
- Information Security Incident Management

Who should attend?:

Experienced information security managers and those who have information security management responsibilities, including IT consultants, auditors, managers, security policy writers, privacy officers, information security officers, network administrators, security device administrators, and security engineers.

GLOBAL
IT TRAINING

Ready to Advance Your Career?
(919) 283-1653
sales@globalittraining.net

CISM: CERTIFIED INFORMATION SECURITY MANAGER

Course Outline:

Domain 1: Information Security Governance

- Develop an information security strategy, aligned with business goals and directives.
- Establish and maintain an information security governance framework.
- Integrate information security governance into corporate governance.
- Develop and maintain information security policies.
- Develop business cases to support investments in information security.
- Identify internal and external influences to the organization.
- Gain ongoing commitment from senior leadership and other stakeholders.
- Define, communicate and monitor information security responsibilities
- Establish internal and external reporting and communication channels.

Domain 2: Information Risk Management

- Establish and/or maintain a process for information asset classification to ensure that measures taken to protect assets are proportional to their business value.
- Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels.
- Ensure that risk assessments, vulnerability assessments and threat analyses are conducted consistently, and at appropriate times, to identify and assess risk to the organization's information.
- Identify, recommend or implement appropriate risk treatment/ response options to manage risk to acceptable levels based on organizational risk appetite.
- Determine whether information security controls are appropriate and effectively manage risk to an acceptable level.
- Facilitate the integration of information risk management into business and IT processes to enable a consistent and comprehensive information risk management program across the organization.
- Monitor for internal and external factors (e.g., threat landscape, cybersecurity, geopolitical, regulatory change) that may require reassessment of risk to ensure that changes to existing or new risk scenarios are identified and managed appropriately.
- Report noncompliance and other changes in information risk to facilitate the risk management decision-making process.
- Ensure that information security risk is reported to senior management to support an understanding of potential impact on the organizational goals and objectives.

Domain 3: Information Security Program Development & Management

- Develop a security program, aligned with information security strategy
- Ensure alignment between the information security program and other business functions
- Establish and maintain requirements for all resources to execute the IS program
- Establish and maintain IS architectures to execute the IS program
- Develop documentation that ensures compliance with policies
- Develop a program for information security awareness and training
- Integrate information security requirements into organizational processes
- Integrate information security requirements into contracts and activities of third parties
- Develop procedures (metrics) to evaluate the effectiveness and efficiency of the IS program
- Compile reports to key stakeholders on overall effectiveness of the IS program and the underlying business processes in order to communicate security performance.

Domain 4: Information Security Incident Management

- Define (types of) information security incidents
- Establish an incident response plan
- Develop processes for timely identification of information security incidents
- Develop processes to investigate and document information security incidents
- Develop incident escalation and communication processes
- Establish teams that effectively respond to information security incidents
- Test and review the incident response plan
- Establish communication plans and processes
- Determine the root cause of IS incidents
- Align incident response plan with DRP and BCP.

GLOBAL
IT TRAINING

Ready to Advance Your Career?
(919) 283-1653
sales@globalittraining.net