CISM Exam Preparation (5 Days)

Information Security Management: ***Managing security to reduce risk and protect the organization***

Course Description:

While information has become more easily accessible and readily available, the associated risks and security threats have not only increased in number, but also complexity. As a result, the importance of ensuring that an enterprise's information is protected has also increased. It is now more important than ever for executives to ensure that their IT security managers have the expertise needed to reduce risk and protect the enterprise.

Designed specifically for information security professionals who are preparing to sit for the CISM exam, the course focuses on the four content areas of the Certified Information Security Manager (CISM) job practice: information security governance, risk management and compliance, information security program development and management, information security incident management. Sample exam items will be used throughout the course to reinforce content and familiarize attendees with the CISM exam question format.

The **CISM** (Certified Information Security Manager) certification is the primary certification for information security professionals who **manage, design, oversee and/or assess** an enterprise's information security.

Every student attending the CISM course progresses through a number of skill checks to ensure knowledge is retained. The instructors for the CISM course are certified with the CISM designation.

Prerequisites:

This course is suitable for anyone looking to prepare for the CISM exam. As Such, there are no prerequisites for either the course or the exam itself.

To apply for the CISM Certification, you must have a minimum of five years of professional information security management experience. If you do not have this experience, you can still take the course, pass the exam and gain the experience later, as long as it is achieved with a period of five years. See ISACA for details.

Course Topics:

- Information Security Governance
- An information security steering group function
- Legal and regulatory issues associated with Internet businesses, global transmissions and transborder data flows
- Common insurance policies and imposed conditions
- Information security process improvement
- Recovery time objectives (RTO) for information resources
- Cost benefit analysis techniques in assessing options for mitigating risks threats and exposures to acceptable levels.
- Security metrics design, development and implementation.
- Information security management due diligence activities and reviews of the infrastructure.
- Events affecting security baselines that may require risk reassessments
- Changes to information security requirements in security plans, test plans and reperformance
- Disaster recovery testing for infrastructure and critical business applications.
- The requirements for collecting and presenting evidence; rules for evidence, admissibility of evidence, quality and completeness of evidence.
- External vulnerability reporting sources
- The key components of cost benefit analysis and enterprise migration plans
- Privacy and tax laws and tariffs, data import/export restrictions, restrictions on cryptography, warranties, patents, copyrights, trade secrets, national security
- CISM information classification methods
- Life-cycle-based risk management principles and practices.
- Cost benefit analysis techniques in assessing options for mitigating risks threats and exposures to acceptable levels.
- Security baselines and configuration management in the design and management of business applications and the infrastructure.
- Acquisition management methods and techniques
- Evaluation of vendor service level agreements, preparation of contracts)
- CISM question and answer review