شهادة مدير أمن المعلومات المعتمد (CISM)

Certified Information Security Manager (CISM)

Course Objectives:

On completion of the CISM exam preparation course, delegates will:

- Ensure that an enterprise's information is protected
- Have the expertise needed to reduce risk and protect the enterprise
- Design, develop, implement and manage an effective security management program
- Establish and maintain an IT governance framework aligned with business objectives
- Identify and manage information security risks
- Have an understanding of the format and structure of the CISM certification exam
- Have knowledge of the various topics and technical areas covered by the exam
- Practice with specific strategies, tips and techniques for taking and passing the exam

Course Outlines:

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.

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.

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.

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.

Audience

This course is intended for individuals who manage, design, oversee and assess an enterprises' information security which includes, but is not limited to the following job roles:

- Information security practitioners
- Information security consultants
- Information security managers
- Security professionals, including those aspiring to attain the CISM designation