Certified Information Security Manager (CISM)

In this course, students will establish processes to ensure that information security measures align with established business needs.

Length Days: 3 | Length Hours: 24

Course Outline

1 - Information Security Governance

- Establish and maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and ongoing management of the information security program
- Establish and maintain an information security governance framework to guide activities that support the information security strategy
- Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program
- Establish and maintain information security policies to communicate management's directives and guide the development of standards, procedures and guidelines
- Develop business cases to support investments in information security
- Identify internal and external influences to the organization (for example, technology, business environment, risk tolerance, geographic location, legal and regulatory requirements) to ensure that these factors are addressed by the information security strategy
- Obtain commitment from senior management and support from other stakeholders to maximize the probability of successful implementation of the information security strategy
- Define and communicate the roles and responsibilities of information security throughout the organization to establish clear accountabilities and lines of authority
- Establish, monitor, evaluate and report metrics (key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs]) to provide management with accurate information regarding the effectiveness of the information security strategy

2 - Information Risk Management and Compliance

- Establish and 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 periodically and consistently to identify risk to the organization's information
- Determine appropriate risk treatment options to manage risk to acceptable levels
- Evaluate information security controls to determine whether they are appropriate and effectively mitigate risk to an acceptable level
- Identify the gap between current and desired risk levels to manage risk to an acceptable level
- Integrate information risk management into business and IT processes (for example, development, procurement, project management, mergers and acquisitions) to promote a consistent and comprehensive information risk management process across the organization
- Monitor existing risk to ensure that changes are identified and managed appropriately
- Report noncompliance and other changes in information risk to appropriate management to assist in the risk management decision-making process

3 - Information Security Program Development and Management

- Establish and maintain the information security program in alignment with the information security strategy
- Ensure alignment between the information security program and other business functions (for example, human resources [HR], accounting, procurement and IT) to support integration with business processes
- Identify, acquire, manage and define requirements for internal and external resources to execute the information security program
- Establish and maintain information security architectures (people, process, technology) to execute the information security program
- Establish, communicate and maintain organizational information security standards, procedures, guidelines and other documentation to support and guide compliance with information security policies
- Establish and maintain a program for information security awareness and training to promote a secure environment and an effective security culture
- Integrate information security requirements into organizational processes (for example, change control, mergers and acquisitions, development, business continuity, disaster recovery) to maintain the organization's security baseline

- Integrate information security requirements into contracts and activities of third parties (for example, joint ventures, outsourced providers, business partners, customers) to maintain the organization's security baseline
- Establish, monitor and periodically report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program

4 - Information Security Incident Management

- Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents to allow accurate identification of and response to incidents
- Establish and maintain an incident response plan to ensure an effective and timely response to information security incidents
- Develop and implement processes to ensure the timely identification of information security incidents
- Establish and maintain processes to investigate and document information security incidents to be able to respond appropriately and determine their causes while adhering to legal, regulatory and organizational requirements
- Establish and maintain incident escalation and notification processes to ensure that the appropriate stakeholders are involved in incident response management
- Organize, train and equip teams to effectively respond to information security incidents in a timely manner
- Test and review the incident response plan periodically to ensure an effective response to information security incidents and to improve response capabilities
- Establish and maintain communication plans and processes to manage communication with internal and external entities
- Conduct post-incident reviews to determine the root cause of information security incidents, develop corrective actions, reassess risk, evaluate response effectiveness and take appropriate remedial actions
- Establish and maintain integration among the incident response plan, disaster recovery plan and business continuity plan