CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA)

Who Should Attend

The CISA designation is a globally recognized certification for IS audit control, assurance and security professionals. Being CISA-certified showcases your audit experience, skills and knowledge, and demonstrates you are capable to assess vulnerabilities, report on compliance and institute controls within the enterprise. CISA has become world-renowned as the standard of achievement for those who assess an organization's information technology and business systems and provide assurance on their availability and sustainability. The CISA Certification was specifically created for professionals with work experience in information systems auditing, control or security that include:

- Security Professionals
- IS/IT Auditors
- IS/IT Consultants
- IS/IT Audit Managers

Course Objectives

Upon successful completion of this course, students will be able to:

- Prepare for and pass the Certified Information Security Manager (CISM) exam
- Develop an information security strategy and plan of action to implement the strategy
- Manage and monitor information security risks
- Build and maintain an information security plan both internally and externally
- Implement policies and procedures to respond to and recover from disruptive and destructive information security events

Course Outline

Day 1 – Information Security Governance

Attendees will understand the broad requirements for effective information security governance, the elements and actions required to develop an information security strategy, and be able to formulate a plan of action to implement this strategy.

- Establish and maintain an information security strategy and align the strategy with corporate governance
- Establish and maintain an information security governance framework
- Establish and maintain information security policies
- Develop a business case

- Identify internal and external influences to the organization
- Obtain management commitment
- Define roles and responsibilities
- Establish, monitor, evaluate and report metrics

Day 2 – Information Risk Management and Compliance

Students will be able to manage information security risks.

- Establish a process for information asset classification and ownership
- Identify legal, regulatory, organizational and other applicable requirements
- Ensure that risk assessments, vulnerability assessments and threat analyses are conducted periodically.
- Determine appropriate risk treatment options.
- Evaluate information security controls
- Identify the gap between current and desired risk levels
- Integrate information risk management into business and IT processes
- Monitor existing risk.
- Report noncompliance and other changes in information risk

Day 3 – Information Security Program Development and Management

Students will be able to develop and manage an information security plan.

- Establish and maintain the information security program
- Ensure alignment between the information security program and other business functions
- Identify, acquire, manage and define requirements for internal and external resources
- Establish and maintain information security architectures
- Establish, communicate and maintain organizational information security standards, procedures, guidelines
- Establish and maintain 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
- Establish, monitor and periodically report program management and operational metrics

Day 4 – Information Security Incident Management

Students will effectively manage information security within an enterprise and develop policies and procedures to respond to and recover from disruptive and destructive information security events.

- Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents
- Establish and maintain an incident response plan

- Develop and implement processes to ensure the timely identification of information security incidents
- Establish and maintain processes to investigate and document information security incidents
- Establish and maintain incident escalation and notification processes
- Organize, train and equip teams to effectively respond to information security incidents
- Test and review the incident response plan periodically
- Establish and maintain communication plans and processes
- Conduct post-incident reviews
- Establish and maintain integration among the incident response plan, disaster recovery plan and business continuity plan