

CERTIFIED INTERNATIONAL INFORMATION SYSTEM AUDITOR (CIISA)

Course	Certified International Information System Auditor/CIISA
Instructor	Certified American Academy Instructor
Descriptions	The credential of a professionals I.S auditor is valuable. This course delves into the unique challenges of managing an audit and the knowledge necessary to complete the task. Information system auditors take up where the financial auditors do not tread-into the design and implementation effectiveness and operation effectiveness of information system. The course will focus on general computer control, application level control auditing as well introducing of risk based management approach. The course is also designed to help candidates familiar with IT audit concepts and rules for regulatory compliance under Sarbanes-Oxely (corporations), Gramm-Leach-Bliley and FFIEC (both financial), FISMA (government), HIPAA (medical records), SCADA (utilities) and other regulators. The course will also help you to become a true management consultant in IT audit field and will help you well prepared for the American Academy examination, which offered by American I.S Audit and control Association. The instructor-led classroom training covers the CISA body of knowledge to build a working understanding of the material. The training course will cover topics such as auditor responsibilities, scope, audit charter, technical material, privacy requirements, for CISA exam preparation. The course has updated the contents to reflect the new subject material of the CISA exam.

Durations	3 Days
Objectives	At the completion of this course, the participants shall have comprehensive understanding and knowledge in Information System and Technology Audit and encompassing such as: • Participants shall obtain an expanded understanding the role of IT auditors in evaluating IT-related operational and control risk and in assessing the appropriateness and adequacy of management control practices and IT-related controls inside participants' organization • Participants shall obtain the capability in conducting IT audit and implement techniques in performing assurance, attestation, and audit engagements • Participants shall obtain an expanded familiarity with the principle references in IT governance, control and security as related to IT audit • Participants shall obtain the working ability to plan, conduct, and report on information technology audits • Participants shall obtain an understanding of the role of IT auditors regarding IT-related compliance and regulatory audits, such as evaluating control standards • Participants shall be prepared and thoroughly confident upon themselves to take CISA professional certificate examination
Target Audience	• IT Managers • Security Managers • Auditing Staffs • IT Operation Staffs
Course Contents and Descriptions	
Module 1: IS Audit Process	Course Contents and Descriptions
Module 2: IT Governance	The class session will focus on IT audit concepts and processes, which includes: review of some of the key fundamentals of IT auditing, including general auditing standards, risk-based auditing, pre-audit objectives, determining scope and audit objectives, and the process of performing an IT audit. The class session will include discussion on IT

3 Days

	performance, controls, control self-assessment, risk analysis, and the objectives of the IT audit or assurance report.
Module 3: System and Infrastructure Life Cycle	The class session shall describe on practical methodology in conducting the effective and efficient IT audit, expand upon the need for appropriate controls and assurance processes for business and IT environment. The participants will be geared toward gaining a working understanding of the content and value of the management guidelines and assurance methodology. Discussion will focus on the importance of measurement in achieving organizational and IT objectives. The session will also focus on the business and IT environments subject to operational and control assessments (audit).
Module 4: IT Service Delivery and Support	Provide assurance that the IT service management practices will ensure delivery of the level of service required to meet the organization's objectives. The module describes as follows: • Evaluate service level management practices to ensure that the level of service from internal and external service providers is defined and managed • Evaluate operations management to ensure that IT support functions effectively meet business needs • Evaluate data administration practices to ensure the integrity and optimization of databases • Evaluate the use of capacity and performance monitoring tools and techniques to ensure that IT services meet the organization's objectives • Evaluate change, configuration and release management practices to ensure that changes made to the organization's production environment are adequately controlled and documented • Evaluate problem and incident management practices to ensure that incidents, problems or errors are recorded, analyzed and resolved in a timely manner • Evaluate the functionality of the IT infrastructure (e.g., network components, hardware, system software) to ensure that it supports the organization's objectives
Module 5: Protection of Information Assets	Provide assurance that the security architecture policies, standards, procedures and controls) ensures the confidentiality, integrity and availability of information assets. The module descriptions are as follows:

	• Evaluate the design, implementation and monitoring of logical access controls to ensure the confidentiality, integrity, availability and authorized use of information assets • Evaluate network infrastructure security to ensure confidentiality, integrity, availability and authorized use of the network and the information transmitted • Evaluate the design, implementation and monitoring of environmental controls to prevent or minimize loss • Evaluate the design, implementation and monitoring of physical access controls to ensure that information assets are adequately safeguarded • Evaluate the processes and procedures used to store, retrieve, transport and dispose of confidential information assets
Module 6: Business Continuity Plan	Provide assurance that in the event of a disruption the business continuity and disaster recovery processes will ensure the timely resumption of IT service, while minimizing the business impacts. The module covers as described below: • Evaluate the adequacy of backup and restore provisions to ensure the availability of information required to resume processing • Evaluate the organization's disaster recovery plan to ensure that it enables the recovery of IT processing capabilities in the event of a disaster • Evaluate the organization's business continuity plan to ensure the organization's ability to continue essential business operations during the period of an IT disruption
Case Studies	Case-based discussions will be conducted with topics related to the subjects of training. Exam exercises and questions evaluation.