



CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL

Course	CRISC
Instructor	American Academy Instructor
Descriptions	The Certified in Risk and Information Systems Control™ certification is designed for IT professionals who have hands-on experience with risk identification, assessment, and evaluation; risk response; risk monitoring; IS control design and implementation; and IS control monitoring and maintenance. The CRISC designation will not only certify professionals who have knowledge and experience identifying and evaluating entity-specific risk, but also aid them in helping enterprises accomplish business objectives by designing, implementing, monitoring and maintaining risk-based, efficient and effective IS controls
Objectives	CRISC course covers how to establish an appropriate infrastructure and culture and apply a logical and systematic method of establishing the context, identifying, analyzing, evaluating, treating, monitoring and communicating IT risks associated with any activity, function or process in a way that will enable organizations to minimize losses and maximize gains. At the completion of this course, the participants should be able to : • Conceptualize organizations risk management within IT processes • Identify and analyze risks within IT operations and understand the implications to the whole business operation • Improve IT operation risk level thru the application and implementation of IT risk management methodology and best practices • Support the attainment of organizational business objectives by providing comprehensive perspective of IT risk management to the executive management of the organization • Plan to implement tool for identifying, analyzing, eradicating and communicating the risks within the cycle of risk management

Target Audience	IT professionals interested in earning Certified in Risk and Information Systems Controls (CRISC) certification. CRISC is for IT professionals, risk professionals, business analysts, project manager and/or compliance professionals, how work towards evaluation and mitigation of risk, and who have job experience in the following areas: • Risk identification, assessment and evaluation; • Risk response and monitoring • IS control design/monitoring and implementation/maintenance
Duration	3 Days
Course Contents and Descriptions	
Segment 1: Risk Identification, Assessment and Evaluation (RI): (31%)	The segment defines Process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives and deciding what countermeasures
Segment 2: Risk Response (RR): (17%)	The participants learn to recognize the following issues in the risk management processes such as: • Following the identification and classification of information resources or assets and the risks implied, risk response plan is constructed • Assess threats and vulnerabilities and the likelihood of their occurrence Identification and classification of information resources or assets that need protection as for creation of the Risk Response • Assess the effectiveness of the Risk Response
Segment 3: Risk Monitoring (RM): (17%)	This segment shall describe on techniques for monitoring and assessment of implemented Risk Response within the cycle of risk management.
Segment 4: Information Systems Controls Design and Implementation :(17%)	The segment shall describe on the mechanism of controls, mapping control to IT assets and IT assets within the perspective of effective control design as related to the operation of information system. Participants shall be guided to identify the suitable and congruent controls as required by



	identified risks, and perform reliable risk-control mapping. •
Segment 5: Information Systems Control Monitoring and Maintenance :(18%)	This segment shall describe to the participants how to establish effective risk management program that covers: • Establish and maintain purpose of the risk management program • Assign the responsibility for the risk management in the information system control monitoring and maintenance
Segment 6: Cases	IT risk management cases