APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

ISACA Certified Risk and Information System Control (CRISC) Training

ISACA Authorized Training · Applied Technology Academy

IT and enterprise risk management is key to an organization's operations and strategy. If you are an Information Technology professional, risk and control professional, business analyst, project manager, or compliance professional, this Certified Risk and Information Systems Control training course will teach you to defend, protect, and future-proof your enterprise.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**4 Days**	**3 years: IS audit, control or security**	**$150,000**	**No**

Course Overview

This official ISACA CRISC training provides you with in-depth coverage on the four CRISC domains: risk identification; IT risk assessment; risk response and mitigation; and risk and control monitoring and reporting.

In this course, you will:

- Prepare for and pass the Certified Risk and Information System Controls (CRISC) exam
- Identify the universe of IT risk to contribute to the execution of the IT risk management strategy
- Analyze and evaluate risk to determine the likelihood and impact on business objectives
- Determine risk response options and evaluate their efficiency and effectiveness to manage risk
- Continuously monitor and report on IT risks and controls

Course Outline

- **Domain 1: IT Risk Identification**
  - 1.1: Collect and review information, including existing documentation, regarding the organization's internal and external business and IT environments to identify potential or realized impacts of IT risk to the organization's business objectives and operations
  - 1.2: Identify potential threats and vulnerabilities to the organization's people, processes, and technology to enable IT risk analysis
  - 1.3: Develop a comprehensive set of IT risk scenarios based on available information to determine the potential impact to business
  - objectives and operations
  - 1.4: Identify key stakeholders for IT risk scenarios to help establish accountability
  - 1.5: Establish an IT risk register to help ensure that identified IT risk scenarios are accounted for and incorporated into the enterprise-wide

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

- **Domain 2: IT Risk Assessment**
  - 2.1: Analyze risk scenarios based on organizational criteria (e.g., organizational structure, policies, standards, technology, architecture, controls) to determine the likelihood and impact of an identified risk
  - 2.2: Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation
  - 2.3: Review the results of risk and control analysis to assess any gaps between current and desired states of the IT risk environment
  - 2.4: Ensure that risk ownership is assigned at the appropriate level to establish clear lines of accountability
  - 2.5: Communicate the results of risk assessments to senior management and appropriate stakeholders to enable risk-based decision making
  - 2.6: Update the risk register with the results of the risk assessment
- **Domain 3: Risk Response and Mitigation**
  - 3.1: Consult with risk owners to select and align recommended risk responses with business objectives and enable informed risk decisions
  - 3.2: Consult with, or assist, risk owners on the development of risk action plans to ensure that plans include key elements (e.g., response, cost, target date)
  - 3.3: Consult on the design and implementation or adjustment of mitigating controls to ensure that the risk is managed to an acceptable level
  - 3.4: Ensure that control ownership is assigned to establish clear lines of accountability
  - 3.5: Assist control owners in developing control procedures and documentation to enable efficient and effective control execution
  - 3.6: Update the risk register to reflect changes in risk and management's risk response
  - 3.7: Validate that risk responses have been executed according to the risk action plans
- **Domain 4: Risk and Control Monitoring and Reporting**
  - 4.1: Define and establish key risk indicators (KRIs) and thresholds based on available data to enable monitoring of changes in risk
  - 4.2: Monitor and analyze key risk indicators (KRIs) to identify changes or trends in the IT risk profile
  - 4.3: Report on changes or trends related to the IT risk profile to assist management and relevant stakeholders in decision making
  - 4.4: Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of control performance
  - 4.5: Monitor and analyze key performance indicators (KPIs) to identify changes or trends related to the control environment and determine the efficiency and effectiveness of controls
  - 4.6: Review the control assessments results to determine the effectiveness of the control environment

- 4.7: Report on the performance of changes to, or trends in the overall risk profile, and control environment to relevant stakeholders to enable decision making

Intended Audience

Designed for those experienced in the management of IT risk and the design, implementation, monitoring, and maintenance of IS controls.

The following professionals benefit the most from CRISC certification:

- Business analysts
- Compliance professionals
- Control professionals
- IT professionals
- Project managers
- Risk professionals
- Anyone tasked with identifying, evaluating, and mitigating organizational risk

Prerequisites

To earn CRISC certification, you must pass the CRISC exam and show three years of experience in the fields of risk management and IS control, per ISACA's requirements.

No experience waivers or substitutions

Follow-On Courses

- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified Data Privacy Solutions Engineer (CDPSE)

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.