ISACA

SIGN IN SUPPORT CAREERS JOIN/REINSTATE MYISACA

Search

WHY ISACA? MEMBERSHIP CREDENTIALING TRAINING & EVENTS RESOURCES ENTERPRISE

STORE

Store | Resources Exam Prep CommunITy Day

Results

Store > Exam Prep > CISA

CISA Online Review Course

$795.00 Member Pricing
$895.00 Non-member Pricing

Add to Order

Description

Prepare to obtain the Certified Information Systems Auditor® (CISA) certification and be recognized among the world's most-qualified information systems professionals. The CISA Online Review Course provides online, on-demand instruction and is ideal for preparing you and fellow audit, assurance, control, security and cyber security professionals for the CISA certification exam.

The course covers all five of the CISA domains, and each section corresponds directly to the CISA job practice. It uses proven instructional design techniques, incorporating an online pre-assessment, narrated interactive eLearning modules, downloadable job aids, and a practice exam. You will be able to navigate the course at your own pace following a recommended structure or target preferred job practice areas. You may also start and stop the course based on your preferred study schedule, picking up exactly where you left off the next time you return.

Learners will have access to the course for one year from date of purchase and will earn 28 CPE upon completion. This course has a seat time of approximately 22 hours and is accessed via the Learning Access tab of your MyISACA dashboard.

Course Description

The CISA Online Review Course is an online preparation course that prepares learners to pass the CISA certification exam using proven instructional design techniques and interactive activities. The course covers all five of the CISA domains, and each section corresponding directly to the CISA job practice.

section corresponding directly to the CISA job practice.

The course incorporates narrated interactive eLearning modules, downloadable job aids, a pre-assessment and practice exam. Learners will be able to navigate the course at their own pace, following a recommended structure, or target preferred job practice areas. Learners may also start and stop the course based on their study schedule, picking up exactly where they left off the next time they access the course.

Learning Objectives:

By the end of this course, you will:

- Gain a better understanding of IS audit and assurance guidelines and standards.
- Develop a working knowledge of the five domains of CISA.

Included Materials:

- Online course
- Downloadable job aids
- Online self-assessment (50 questions)
- Online practice exam (75 questions)

Ideal For:

- Professionals preparing to become CISA certified
- Financial auditors moving into IT audit
- IT generalists moving into IT audit
- Mid-level career change
- Students or recent graduates

Cancellation/Refund Policy

All purchases of online learning courses are final. Access to the online learning courses and materials is immediate upon purchasing; therefore no refunds or exchanges will be provided. Prices subject to change without notice.

Enterprise Training

Enterprise Training

Online review courses are also available for purchase through our enterprise sales team for larger organizations. Visit the Enterprise Training page and reach out to an associate for more information.

Course Outline

Domain 1 — Information System Auditing Process

- Plan an audit to determine whether information systems are protected, controlled, and provide value to the organization.
- Conduct an audit in accordance with IS audit standards and a risk-based IS audit strategy.
- Communicate audit progress, findings, results and recommendations to stakeholders.
- Conduct audit follow-up to evaluate whether risk has been sufficiently addressed.
- Evaluate IT management and monitoring of controls.
- Utilize data analytics tools to streamline audit processes.
- Provide consulting services and guidance to the organization in order to improve the quality and control of information systems.
- Identify opportunities for process improvement in the organization’s IT policies and practices.

Domain 2 – Governance & Management of IT

- Evaluate the IT strategy for alignment with the organization’s strategies and objectives.
- Evaluate the effectiveness of IT governance structure and IT organizational structure.
- Evaluate the organization’s management of IT policies and practices.
- Evaluate the organization’s IT policies and practices for compliance with regulatory and legal requirements.
- Evaluate IT resource and portfolio management for alignment with the organization’s strategies and objectives.
- Evaluate the organization’s risk management policies and practices.
- Evaluate IT management and monitoring of controls.
- Evaluate the monitoring and reporting of IT key performance indicators (KPIs).
- Evaluate whether IT supplier selection and contract management processes align with business requirements.

- Evaluate whether IT supplier selection and contract management processes align with business requirements.
- Evaluate whether IT service management practices align with business requirements.
- Conduct periodic review of information systems and enterprise architecture.
- Evaluate data governance policies and practices.
- Evaluate the information security program to determine its effectiveness and alignment with the organization’s strategies and objectives.
- Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices

Domain 3 – Information Systems Acquisition, Development, & Implementation

- Evaluate whether the business case for proposed changes to information systems meet business objectives.
- Evaluate the organization’s project management policies and practices.
- Evaluate controls at all stages of the information systems development life cycle.
- Evaluate the readiness of information systems for implementation and migration into production.
- Conduct post-implementation review of systems to determine whether project deliverables, controls and requirements are met.
- Evaluate change, configuration, release, and patch management policies and practices.

Domain 4 – Information Systems Operations and Business Resilience

- Evaluate the organization’s ability to continue business operations.
- Evaluate whether IT service management practices align with business requirements.
- Conduct periodic review of information systems and enterprise architecture.
- Evaluate IT operations to determine whether they are controlled effectively and continue to support the organization’s objectives.
- Evaluate IT maintenance practices to determine whether they are controlled effectively and continue to support the organization’s objectives.
- Evaluate database management practices.
- Evaluate data governance policies and practices.

- Evaluate IT maintenance practices to determine whether they are controlled effectively and continue to support the organization’s objectives.
- Evaluate database management practices.
- Evaluate data governance policies and practices.
- Evaluate problem and incident management policies and practices.
- Evaluate change, configuration, release, and patch management policies and practices.
- Evaluate end-user computing to determine whether the processes are effectively controlled.

Domain 5 – Protection of Information Assets

- Conduct audit in accordance with IS audit standards and a risk-based IS audit strategy.
- Evaluate problem and incident management policies and practices.
- Evaluate the organization’s information security and privacy policies and practices.
- Evaluate physical and environmental controls to determine whether information assets are adequately safeguarded.
- Evaluate logical security controls to verify the confidentiality, integrity, and availability of information.
- Evaluate data classification practices for alignment with the organization’s policies and applicable external requirements.
- Evaluate policies and practices related to asset life cycle management.
- Evaluate the information security program to determine its effectiveness and alignment with the organization’s strategies and objectives.
- Perform technical security testing to identify potential threats and vulnerabilities.
- Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices.

Contact Us | Terms | Privacy | Cookie Notice | Fraud Reporting | Bug Reporting | COVID-19

1700 E. Golf Road, Suite 400, Schaumburg, Illinois 60173, USA | +1-847-253-1545 | ©2022 ISACA. All rights reserved.

Document title: Store - CISA Online Review Course - ISACA Portal
Capture URL: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9xEAC
Capture timestamp (UTC): Mon, 13 Jun 2022 14:34:03 GMT

Page 5 of 5