

Updated on 07/28/2026

Sign Up

CRISC Certification Training

4 days (28 hours)

Overview

ISACA's CRISC certification validates recognized expertise in IT risk management, governance, and security controls. It is designed for professionals who want to establish a robust risk management framework aligned with industry expectations and the official exam.

Our CRISC Certification training provides targeted preparation for the official exam, with a curriculum designed to reinforce key concepts from the certification framework and apply them to real-world scenarios.

You will learn to analyze business risks, assess threats and vulnerabilities, define risk responses, and manage the metrics and reporting required within a governance framework.

The course also emphasizes understanding the four CRISC domains, the exam's structure, the types of questions, and the methodological approaches needed to answer accurately and effectively.

Upon completion of this course, you will have a structured understanding of risk governance, controls, and ISACA best practices, enabling you to approach the exam methodically and with confidence.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Understand the scope and requirements of the CRISC certification.

- Master the four domains of the official framework and how they relate to one another.
- Analyze risks, impacts, and mitigation priorities.
- Select risk responses tailored to governance and compliance challenges.
- Effectively prepare for the exam format through targeted practice scenarios.

Target Audience

- Cybersecurity Auditor
- Risk manager
- Information Security Manager
- GRC Consultant
- Internal Auditor

Prerequisites

- Basic knowledge of cybersecurity and risk management.
- Professional experience in an IT, audit, or security environment.
- Understanding of governance and compliance issues.
- Practical experience with internal control and incident management concepts.

Technical Prerequisites

- A recent computer with an up-to-date browser and a screen large enough to comfortably view course materials.
- A stable Wi-Fi or Ethernet connection for remote sessions and live discussions.
- A microphone and headset or headphones to ensure good audio quality during video conferences.
- A standard office environment with PDF, Excel, or equivalent software for exercises and answer keys.
- If the session is conducted remotely, a second screen can make it easier to follow along with the course materials and workshops.

CRISC Training Program

[Day 1 - Morning]

Fundamentals of the Certification

- Overview of the CRISC certification, its objectives, and how it enhances professional value.
- Review of the official reference framework, the four domains, and the competencies assessed on the exam.
- Overview of the governance, risk, control, and reporting framework.
- Mapping of exam expectations and the most common pitfalls in understanding the material.
- Organization of the four-day preparation program, including a review strategy and learning priorities.
- Hands-on workshop: initial assessment of skill level and identification of areas needing improvement.

[Day 1 – Afternoon] Governance

and Business Context

- Understanding the role of risk governance within the organization and its links to strategy.
- Identify roles, responsibilities, and lines of defense within a risk management framework.
- Link business objectives, internal policies, and regulatory requirements.
- Analyze risk appetite, risk tolerance, and associated decision-making criteria.
- Examine the concepts of control frameworks, prioritization, and steering.
- Hands-on workshop: guided analysis of a business case and assessment of governance issues.

[Day 2 - Morning]

Risk Identification and Assessment

- Master the steps for identifying assets, threats, vulnerabilities, and risk scenarios.
- Distinguish between qualitative and quantitative approaches to risk assessment.
- Assess the impact, likelihood, and level of criticality within a business context.
- Structure a risk analysis consistent with the organization's objectives.
- Understand the relationships between inherent risk, residual risk, and acceptable risk levels.
- Hands-on workshop: building a risk matrix based on a realistic scenario.

[Day 2 - Afternoon]

Risk Response and Mitigation

- Compare risk treatment strategies: accept, reduce, transfer, or avoid.
- Define appropriate controls based on cost, effectiveness, and the target level of residual risk.
- Incorporate the concepts of action plans, prioritization, and ongoing monitoring.
- Assess the expected effects of security and governance measures.
- Link risk management to continuity and resilience requirements.
- Hands-on workshop: Justified selection of a risk treatment strategy for several use cases.

[Day 3 - Morning]

Controls and Monitoring

- Understand the role of controls in reducing and managing risk.
- Identify preventive, detective, and corrective controls within an operational system.
- Link monitoring mechanisms to management and alert requirements.
- Analyze performance and risk indicators to monitor the effectiveness of the measures.
- Examine the required documentation, evidence, and traceability of controls.
- Hands-on workshop: reviewing a control framework and identifying gaps in coverage.

[Day 3 - Afternoon] Reporting

and Communication

- Structure risk reports that are clear, useful, and tailored to decision-makers.
- Present analysis results with the appropriate levels of summary and detail.
- Tailor your communication to stakeholders, including management, business units, audit, and security.
- Understand the role of dashboards, alerts, and remediation plans.
- Review the concepts of compliance, escalation, and crisis communication.
- Hands-on workshop: drafting a risk summary for a steering committee.

[Day 4 - Morning]

Targeted exam preparation

- Review the key points of the four domains using active memorization techniques.
- Identify recurring phrasing in CRISC questions and best practices for reading them.
- Practice deciding between similar answer choices and justifying the best choice.
- Improve time management and the method for eliminating distractors.
- Consolidate ISACA vocabulary and frequently tested concepts.
- Hands-on workshop: a series of practice questions with answers and group debriefing.

[Day 4 - Afternoon]

Final review and mock exam

- Conduct a final review of key concepts and common mistakes.
- Take a practice exam under conditions similar to the certification exam.
- Analyze answers, expected responses, and key points to watch for by subject area.
- Develop a personalized review strategy leading up to the exam.
- Prepare for final adjustments to your study methods and stress management.
- Hands-on workshop: full mock exam followed by a detailed review of the answers.

Target Companies

This training is intended for both individuals and companies—large or small—that wish to train their teams in new, advanced IT technologies or to acquire specific professional knowledge or modern methods.

Entry-Level Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us

assess their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.