301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

View Full Course Details including Latest Schedule Online

ISACA

CRISC (Certified in Risk and Information Systems Control)

BONUS! Cyber Phoenix Subscription Included: All Phoenix TS students receive complimentary ninety (90) day access to the Cyber Phoenix learning platform, which hosts hundreds of expert asynchronous training courses in Cybersecurity, IT, Soft Skills, and Management and more!

Course Overview

Phoenix TS' 3-day CRISC (Certified in Risk and Information Systems Control) training and certification boot camp in Washington, DC Metro, Tysons Corner, VA, Columbia, MD or Live Online provides you the necessary knowledge and skills to properly understand, mitigate and manage risk within an organization.

In addition, students will be led through all the exam objectives so that they are properly prepared to handle the CRISC certification exam at the end of the course.

CRISC certification exams can now be taken via online remote proctored

What You'll Learn

- Risk Identification, Assessment and Evaluation
- Information Security Control Design and Implementation
- Risk Response
- IS Control Monitoring and Maintenance
- Risk Monitoring

DATE	LOCATION	
7/22/24 - 7/26/24 (3 days)	**Live Online** Open	Contact Us
7/22/24 - 7/26/24 (3 days)	**Columbia, MD** Open	Contact Us

Who Should Attend

- Chief Audit Executives
- Audit Partners/Heads
- CEOs/CFOs
- CIOs/CISOs
- Chief Compliance/Privacy/Risk Officers
- Security Managers/Directors/Consultants

Prerequisites

We recommend at least (3) three years of work experience performing tasks across at least three of the CRISC domains

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

THE CRISC DIFFERENCE

Whether you are seeking a new career opportunity or striving to grow within your current organization, a CRISC certification proves your expertise in these work-related domains:



Exam Information

CRISC Exam Details:

The CRISC exam measures skills within the Following Domains:

- Domain 1 – IT Risk Identification – (27%)
- Domain 2 – IT Risk Assessment – (28%)
- Domain 3 – Risk Response Mitigation – (23%)
- Domain 4 – Risk and Control Monitoring and Reporting – (22%)

All ISACA certification exams consist of 150 multiple choice questions that cover the respective job practice areas created from the most recent job practice analysis.

You have 4 hours to complete the exam

CRISC Certification Exam Price:

Member $575

Non Member $760

Recertification

The CRISC continuing professional education (CPE) policy requires that you attain at least 20 CPE hours per year and 120 CPE hours every three years.

Duration

3 Days

Program Level

Advanced

Training Delivery Methods

Group Live

Duration

5 Days / 32 hours Training

CPE credits

26 NASBA CPE Credits

Field of Study

Information Technology

Advanced Prep

N/A

Course Registration

Candidates can choose to register for the course by via any of the below methods:

- Email: Sales@phoenixts.com
- Phone: 301-582-8200
- Website: www.phoenixts.com

Upon registration completion candidates are sent an automated course registration email that includes attachments with specific information on the class and location as well as pre-course study and test preparation material approved by the course vendor. The text of the email contains a registration confirmation as well as the location, date, time and contact person of the class.

Online enrolment closes three days before course start date.

On the first day of class, candidates are provided with instructions to register with the exam provider before the exam date.

Complaint Resolution Policy

To view our complete Complaint Resolution Policy policy please click here: Complaint Resolution Policy

Refunds and Cancellations

To view our complete Refund and Cancellation policy please click here: Refund and Cancellation Policy

Course Outline

Domain 1—IT Risk Identification

Identify the universe of IT risk to contribute to the execution of the IT risk management strategy in support of business objectives and in alignment with the enterprise risk management (ERM) strategy.

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 risk profile.
1.6 Identify risk appetite and tolerance defined by senior leadership and key stakeholders to ensure alignment with business objectives.
1.7 Collaborate in the development of a risk awareness program, and conduct training to ensure that stakeholders understand risk and to promote a risk-aware culture.

Domain 2—IT Risk Assessment

Analyze and evaluate IT risk to determine the likelihood and impact on business objectives to enable risk-based decision making.

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 Mitigation

Determine risk response options and evaluate their efficiency and effectiveness to manage risk in alignment with business objectives.

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

Continuously monitor and report on IT risk and controls to relevant stakeholders to ensure the continued efficiency and effectiveness of the IT risk management strategy and its alignment to business objectives.

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 results of control assessments 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.

BONUS! Cyber Phoenix Subscription Included: All Phoenix TS students receive complimentary ninety (90) day access to the Cyber Phoenix learning platform, which hosts hundreds of expert asynchronous training courses in Cybersecurity, IT, Soft Skills, and Management and more!

Phoenix TS is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints re-garding registered sponsors may be submitted to the National Registry of CPE Sponsors through its web site: www.nasbaregistry.org

Starting at **$2,195**

ATTENTION

For GSA pricing or Contractor quotes call

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

301-258-8200 – Option 2.

GSA

Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.

This CRISC **Certification Training** course includes:

- 3 days of expert training by a certified CRISC instructor
- Required course materials such books and other materials
- Sample exam questions
- Breakfast, which includes a combination of bagels, doughnuts, yogurt, fruit and juices*
- Soda/Coffee/Tea, which are available throughout the day*
- Fresh baked cookies are available in the afternoon*
- Course Retake option

**denotes this benefit is only available at participating locations.*