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

View Full Course Details including Latest Schedule Online

(ISC)²

# CGRC (Certified in Governance, Risk and Compliance)

Earning the ISC2 CGRC *formerly CAP* certification is a key factor in advancing within your Information Security career; it verifies an individual's skills and knowledge for implementing Risk Management Framework, identifying security controls and vulnerabilities for measuring organizational risks.

**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

Official ISC2 Training Seminar for the CGRC (Certified in Governance, Risk and Compliance) *formerly known as CAP* provides a comprehensive review of the knowledge required for authorizing and maintaining information systems within the NIST Risk Management Framework. This training course will help students review and refresh their knowledge and identify areas they need to study for the CGRC exam. Content aligns with and comprehensively covers the seven domains of the (ISC)² CGRC Common Body of Knowledge (CBK®).

Official courseware is developed by (ISC)² – creator of the CGRC CBK – to ensure your training is relevant and up-to-date. Our instructors are verified security experts who hold the CGRC and have completed intensive training to teach (ISC)² content. At the completion of this course, participants will be able to:

- Identify and describe the steps and tasks within the NIST Risk Management Framework (RMF).
- Apply common elements of other risk management frameworks using the RMF as a guide.
- Describe the roles associated with the RMF and how they are assigned to tasks within the RMF.

- Execute tasks within the RMF process based on assignment to one or more RMF roles.
- Explain organizational risk management and how it is supported by the RMF.

## Schedule

| DATE | LOCATION | |
|---|---|---|
| 4/29/24 - 5/03/24 (5 days) | Columbia, MD Open | Contact Us |
| 5/06/24 - 5/10/24 (5 days) | Live Online Open | Contact Us |
| 6/10/24 - 6/14/24 (5 days) | Live Online Open | Contact Us |
| 7/22/24 - 7/26/24 (5 days) | Columbia, MD Open | Contact Us |
| 7/29/24 - 8/02/24 (5 days) | Live Online Open | Contact Us |
| 9/16/24 - 9/20/24 (5 days) | Live Online Open | Contact Us |
| 10/28/24 - 11/01/24 (5 days) | Columbia, MD Open | Contact Us |
| 11/11/24 - 11/15/24 (5 days) | Live Online Open | Contact Us |
| 2/03/25 - 2/07/25 (5 days) | Columbia, MD Open | Contact Us |
| 2/03/25 - 2/07/25 (5 days) | Live Online Open | Contact Us |

## 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

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

# Refunds and Cancellations

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

# Course Outline

## Chapter 1: Prepare (10 Modules)

- Explain the purpose and value of preparation.
- Identify references associated with the Prepare step.
- Identify other risk management frameworks and their relationship to RMF tasks.
- Identify relevant security and privacy regulations.
- List the references, processes and outcomes that define:

- RMF Task P-1: Risk Management Roles
- RMF Task P-2: Risk Management Strategy
- RMF Task P-3: Risk Assessment – Organization
- RMF Task P-14: Risk Assessment – System
- RMF Task P-4: Organizationally Tailored Control Baselines and Cybersecurity Framework Profiles
- RMF Task P-5: Common Control Identification
- RMF Task P-6: Impact-Level Prioritization
- RMF Task P-7: Continuous Monitoring Strategy – Organization
- RMF Task P-8: Mission or Business Focus
- RMF Task P-9: System Stakeholders
- RMF Task P-10: Asset Identification
- RMF Task P-11: Authorization Boundary
- RMF Task P-12: Information Types
- RMF Task P-13: Information Life Cycle
- RMF Task P-15: Requirements Definition
- RMF Task P-16: Enterprise Architecture
- RMF Task P-17: Requirements Allocation
- RMF Task P-18: System Registration

- Complete selected Prepare Tasks for the example system.

## Chapter 2: Categorize (5 Modules)

- Explain the purpose and value of categorization.
- Identify references associated with the Categorize step.
- List the references, processes, and outcomes that define Risk Management Framework (RMF) Task

C-1: System Description.
- Describe a system's architecture.
- Describe an information system's purpose and functionality.
- Describe and document a system's characteristics.
- List the references, processes and outcomes that define RMF Task C-2: Security Categorization.
- Categorize an information system.
- List the references, processes and outcomes that define RMF Task C-3: Security Categorization Review and Approval.
- Describe the review and approval process for security categorization.
- Categorize the example systems.

## Chapter 3: Select (7 Modules)

- Explain the purpose and value of control selection and allocation.
- Identify references associated with the Select step.
- Relate the ISO 27001 Statement of Applicability to the NIST RMF.
- List the references, processes and outcomes that define RMF Task S-1: Control Selection.
- List the references, processes and outcomes that define RMF Task S-2: Control Tailoring.
- Select appropriate security control baselines based on organizational guidance.
- Tailor controls for a system within a specified operational environment.
- List the references, processes and outcomes that define RMF Task S-3: Control Allocation.
- List the references, processes and outcomes that define RMF Task S-4: Documentation of Planned Control Implementations.
- Allocate security and privacy controls to the system and to the environment of operation.
- Document the controls for the system and environment of operation in security and privacy plans.
- List the references, processes and outcomes that define RMF Task S-5: Continuous Monitoring Strategy – System.
- Develop and implement a system-level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy.
- List the references, processes and outcomes that define RMF Task S-6: Plan Review and Approval.
- Review and approve the security and privacy plans for the system and the environment of operation.
- Allocate security controls for the example system.
- Tailor security controls for the example system.
- Draft a continuous monitoring plan for the example system.

## Chapter 4: Implement (5 Modules)

- Explain the purpose and value of implementation.
- Identify references associated with the Implement step.
- List the references, processes and outcomes that define RMF Task I-1: Control Implementation.

- Identify appropriate implementation guidance for control frameworks.
- Integrate privacy requirements with system implementation.
- List the references, processes and outcomes that define RMF Task I-2: Update Control Implementation Information.
- Update a continuous monitoring strategy.
- Update a control implementation plan.

## Chapter 5: Assess (6 Modules)

- Explain the purpose and value of assessment.
- Identify references associated with the Assess step.
- Understand and identify common elements of the NIST process that are included in other frameworks and processes.
- List the references, processes and outcomes that define RMF Task A-1: Assessor Selection.
- List the references, processes and outcomes that define RMF Task A-2: Assessment Plan.
- List the references, processes and outcomes that define RMF Task A-3: Control Assessment.
- List the references, processes and outcomes that define RMF Task A-4: Assessment Reports.
- List the references, processes and outcomes that define RMF Task A-5: Remediation Actions.
- List the references, processes and outcomes that define RMF Task A-6: Plan of Action and Milestones.
- Develop an assessment plan for identified controls in the example system.
- Develop a remediation plan for unsatisfied controls in the example system.

## Chapter 6: Authorize (6 Modules)

- Explain the purpose and value of authorization.
- Identify references associated with the Authorize step.
- Relate system approvals under organizational processes to the concepts applied in the NIST RMF.
- List the references, processes and outcomes that define RMF Task R-1: Authorization Package.
- List the references, processes and outcomes that define RMF Task R-2: Risk Analysis and Determination.
- List the references, processes and outcomes that define RMF Task R-3: Risk Response.
- List the references, processes and outcomes that define RMF Task R-4: Authorization Decision.
- List the references, processes and outcomes that define RMF Task R-5: Authorization Reporting.
- Develop a risk determination for the example system on the system risk level.
- Authorize the system for operation.
- Determine appropriate elements for the Authorization decision document for the example system.

## Chapter 7: Monitor (8 Modules)

- Explain the purpose and value of monitoring.

- Identify references associated with the Monitor step.
- List the references, processes and outcomes that define RMF Task M-1: System and Environment Changes.
- (Coordinate) Integrate cybersecurity risk management with organizational change management.
- List the references, processes and outcomes that define RMF Task M-2: Ongoing Assessments.
- Monitor risks associated with supply chain.
- List the references, processes and outcomes that define RMF Task M-3: Ongoing Risk Response.
- Understand elements for communication surrounding a cyber event.
- List the references, processes and outcomes that define RMF Task M-4: Authorization Package Updates.
- List the references, processes and outcomes that define RMF Task M-5: Security and Privacy Reporting.
- List the references, processes and outcomes that define RMF Task M-6: Ongoing Authorization.
- List the references, processes and outcomes that define RMF Task M-7: System Disposal.
- Discuss Monitor step activities in the example system.

### Chapter 8: CGRC Certification Information

This chapter covers important information about the experience requirements for the CGRC certification and ISC2 exam policies and procedures. Details were based on information as of August 2021. It is recommended that learners go to the $(ISC)^2$ website www.isc2.org for the most up-to-date information on certification requirements and the exam process.

## Exam Information

### CGRC Certification Exam Overview:

The CGRC (formerly known as CAP) exam will test the breadth and depth of a student's knowledge by primarily focusing on the seven domains which make up the topics of CGRC CBK, taxonomy of information security:

1. Information Security Risk Management Program (15%)
2. Categorization of Information Systems (IS) (13%)
3. Selection of Security Controls (13%)
4. Implementation of Security Controls (15%)
5. Assessment of Security Controls (14%)
6. Authorization of Information Systems (IS) (14%)
7. Continuous Monitoring (16%)

## CGRC Certification Exam Details:

- Questions on the Exam: 125
- Score Needed to Pass: at least 700/1,000
- Duration of the Exam: 3 Hours
- Format of the Exam: multiple choice
- Delivery Details: The CGRC exam is offered through the global network of Pearson VUE testing centers as a computer-based test.

## Finance your CGRC Training!

We have partnered with Meritize to provide our students with financing options to fund your education. Check your loan options in minutes without impacting your credit score. Click here to apply




## CGRC Certification Training FAQs

### Who should take this class?

This certification is sought after by Authorization Officials, Information System Security Officers, Information Owners, System Owners and Senior System Managers.

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

## What is the average salary with an (ISC)² CGRC Certification?

According to payscale.com, professionals with the CGRC certification earn an average salary of $100,000.

**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 **$3,124**

**ATTENTION**

For GSA pricing or Contractor quotes call 301-258-8200 – Option 2.

GSA

10420 Little Patuxent Parkway Suite 500 Columbia, MD 21044

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



## Price Match Guarantee

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

## This **CAP Certification Training** course includes:

- 5 days of instructor-led training
- ISC2 CGRC Certification Exam voucher
- ISC2 CGRC practice exams
- ISC2 CGRC official CBK
- ISC2 CGRC Certification Training book
- Pre and post assessments
- CGRC onsite exam scheduling
- Certificate of completion for up to 40 CEUs/CPEs to be used toward renewing relevant certifications
- CGRC course retake guarantee
- CGRC certification satisfies DOD 8570 IAM Level II
- Notepad, pen and highlighter
- Variety of bagels, fruits, doughnuts and cereal available at the start of class*
- Tea, coffee and soda available throughout the day*
- Freshly baked cookies every afternoon*

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