Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

CGRC Certified in Governance, Risk and Compliance Training Course

Course Description

SecureNinja's Certified in Governance, Risk, and Compliance (CGRC) training and certification course covers the exam objectives that measure the knowledge, skills, and abilities required for personnel involved in the process of authorizing and maintaining information systems within the Risk Management Framework (RMF). Specifically, this credential applies to those responsible for formalizing processes used to assess risk and establish security requirements and documentation. Their decisions will ensure those information systems possess security commensurate with the level of exposure to potential risk, as well as damage to assets or individuals. The CGRC is the only certification under the DoD8570 mandate that aligns with each RMF step. It shows employers you have the advanced technical skills and knowledge to authorize and maintain information systems within the RMF using best practices, policies, and procedures established by the cybersecurity experts at (ISC)². The 4-day immersive boot camp covers all of the latest exam objectives complete with 400+ up-to-date exam questions in SecureNinja's Student Portal Quiz Engine.

Topics Covered

The CGRC examination tests the breadth and depth of a candidate’s knowledge by focusing on the seven domains which comprise the CGRC CBK® taxonomy of information security topics:

- Domain 1: Security and Privacy Governance, Risk Management, and Compliance Program
- Domain 2: Scope of the System
- Domain 3: Selection and Approval of Framework, Security, and Privacy Controls
- Domain 4: Implementation of Security and Privacy Controls
- Domain 5: Assessment/Audit of Security and Privacy Controls
- Domain 6: System Compliance
- Domain 7: Compliance Maintenance

The credential is appropriate for commercial markets, civilian and local governments, and the U.S. Federal government including the State Department and the Department of Defense (DoD). Job functions such as authorization officials, system owners, information owners, information system security officers, and certifiers, as well as all senior system managers, apply.

Course Outline

Day 1: Foundations of Governance, Risk, and Compliance

•Introduction to CGRC & Course Overview

- **Security and Privacy Governance, Risk Management, and Compliance Program**

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

•Governance, risk management, and compliance principles

•Regulatory frameworks (NIST, COBIT, ISO/IEC)

•System Development Life Cycle (SDLC) and compliance integration

•Roles and responsibilities in compliance

• **Scope of the System**

•Defining system boundaries and scope

•Information classification and security objectives

•Assessing impact levels based on compliance requirements

•**Practical Exercise:** Case Study – Defining Scope for an Information System

Day 2: Control Selection, Implementation, and Compliance Strategies

• **Selection and Approval of Framework, Security, and Privacy Controls**

•Identifying and documenting baseline controls

•Tailoring security controls to organizational needs

•Developing a continuous monitoring strategy

• **Implementation of Security and Privacy Controls**

•Implementing security and privacy controls effectively

•Ensuring alignment with compliance mandates

•Managing residual risks

•**Practical Exercise:** Developing a Security Control Implementation Plan

Day 3: Assessment, Auditing, and System Compliance

• **Assessment/Audit of Security and Privacy Controls**

•Preparing for security assessments and audits

•Compliance verification and validation techniques

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

•Conducting assessments and reporting findings

• **System Compliance**

•Documenting compliance efforts

•Risk acceptance and treatment options

•Stakeholder involvement and decision-making

•**Practical Exercise:** Conducting a Compliance Audit and Risk Assessment

Day 4: Maintaining Compliance & Final Review

• **Compliance Maintenance**

•Continuous monitoring and control evaluation

•Adapting to evolving security and privacy requirements

•Updating policies and procedures

• **Exam Preparation & Review**

•Key takeaways from each domain

•Sample questions and test-taking strategies

•Final Q&A and discussion

Prerequisites

The ideal candidate should have experience, skills, or knowledge in any of the following areas:

- IT Security
- Information Assurance
- Information Risk Management
- Certification
- Systems Administration
- One - two years of general technical experience
- Two years of general systems experience
- One - two years of database/systems development/network experience
- Information Security Policy
- Technical or auditing experience within government, the U.S. Department of Defense, the financial or health care industries, and/or auditing firms
- Strong familiarity with NIST documentation

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

Required Exam

ISC2 CGRC Exam

- Format: 125 multiple-choice questions.
- Duration: 3 hours.
- Passing Score: 700 out of 1000 points.

Course Length

- 4 Days
- 32 Hours

Follow-on Courses

CISSP