INFOSECTRAIN

# CGRC

Certified in Governance, Risk & Compliance Training (Formerly CAP )

INFOSECTRAIN

# COURSE HIGHLIGHTS

INFOSECTRAIN

# COURSE OVERVIEW

InfosecTrain's CGRC: Certified in Governance, Risk, and Compliance (Formerly CAP ) Training Course is a comprehensive program tailored to showcase participant's competence in effectively integrating governance, performance management, risk management, and regulatory compliance into the organization's operations. This course comprehensively covers seven essential domains, initiating the development of a robust information security risk management program. Following this, it thoroughly explores defining the scope of the information system. Participants are then skillfully guided through the processes of selection and approval of security and privacy controls, along with their effective Implementation. A significant emphasis is placed on the assessment and audit of these controls to ensure their efficacy.

The course further delves into the authorization and approval processes pertinent to information systems and concludes with detailed strategies for continuous monitoring. This curriculum is meticulously crafted to provide participants with a holistic understanding of how governance, risk, and compliance are integrated within an organizational framework, making it an indispensable course for professionals striving to master these critical domains.

INFOSECTRAIN

# Why CGRC with InfosecTrain?

InfosecTrain is a leading IT security training and consulting organization offering best-in-class yet cost-effective, customized training programs to enterprises and individuals across the globe. We offer role-specific certification training programs and prepare professionals for the future. Our CGRC: Certified in Governance, Risk, and Compliance (Formerly CAP ) Training Course employs various frameworks to incorporate security and privacy in line with organizational goals, thus empowering stakeholders to make knowledgeable choices about data security, compliance, managing risks in the supply chain, and other related areas.

Here's what you get when you choose InfosecTrain as your learning partner:

- **Flexible Schedule:** Training sessions to match your schedule and accommodate your needs.
- **Post Training Support with No Expiry Date:** Ongoing assistance and support until the learners achieve their certification goals.
- **Recorded Sessions:** Access to LMS or recorded sessions for post-training reference.
- **Customized Training:** A training program that caters to your specific learning needs.
- **Knowledge Sharing Community:** Collaborative group discussions to facilitate knowledge sharing and learning.
- **Certificate:** Each candidate receives a certificate of participation as a testament to their accomplishment.
- **Expert Career Guidance:** Free career guidance and support from industry experts.

INFOSECTRAIN

# Target Audiences:

- Cybersecurity Auditor
- Cybersecurity Compliance Officer
- GRC Architect
- GRC Manager
- Cybersecurity Risk and Compliance Project Manager
- Cybersecurity Risk and Controls Analyst
- Cybersecurity Third-Party Risk Manager
- Enterprise Risk Manager
- GRC Analyst
- GRC Director
- Information Assurance Manager

# Prerequisites:

- **Minimum Requirement:** Two years of full-time experience in one or more domains of the CGRC exam outline.
- **Alternative Experience:** Part-time work and internships can contribute to the experience requirement.
- **Associate Path:** Without the required experience, pass the CGRC exam to become an Associate of (ISC)².
- **Timeframe for Associates:** Associates must gain two years of experience within three years.

# Note:

- CGRC® is a registered mark of The International Information Systems Security Certification Consortium (ISC)².
- We are not an authorized training partner of (ISC)².

INFOSECTRAIN

# Exam Information

| | |
|---|---|
| **Exam Duration** | 3 Hours |
| **Number of Questions** | 125 |
| **Exam Format** | Multiple-choice |
| **Passing Score** | 700 out of 1000 |
| **Exam Language** | English |

INFOSECTRAIN

# Course Objectives

You will be able to:

- Understand foundational principles, risk management frameworks, system development life cycle, and roles in authorization processes.
- Define system scope architecture and categorize information types and impact levels.
- Identify baseline controls, tailor controls to systems, develop continuous monitoring strategies, and review security plans.
- Implement and document selected controls, ensuring alignment with organizational architecture.
- Prepare and conduct assessments/audits, analyze results, propose remediation actions, and develop final reports and action plans.
- Compile authorization documentation, assess system risk, and formalize the authorization process.
- Monitor system changes, conduct ongoing assessments, review supply chain risks, participate in response planning, update monitoring strategies, and report on risk posture.

INFOSECTRAIN

# CGRC Course Content

- **Domain 1:** Information Security Risk Management Program (16%)
- **Domain 2:** Scope of the Information System (11%)
- **Domain 3:** Selection and Approval of Security and Privacy Controls (15%)
- **Domain 4:** Implementation of Security and Privacy Controls (16%)
- **Domain 5:** Assessment/Audit of Security and Privacy Controls (16%)
- **Domain 6:** Authorization/Approval of Information Systems (10%)
- **Domain 7:** Continuous Monitoring (16%)

INFOSECTRAIN

## Domain 1: Information Security Risk Management Program (16%)

### 1.1: Understand the Foundation of an Organization Information Security Risk Management Program

- Principles of information security
- Risk management frameworks (e.g., National Institute of Standards and Technology (NIST), cyber security framework, Control Objectives for Information and Related Technology (COBIT), International Organization for Standardization (ISO) 27001, International Organization for Standardization (ISO) 31000)
- System Development Life Cycle (SDLC)
- Information system boundary requirements
- Security controls and practices
- Roles and responsibilities in the authorization/approval

### 1.2: Understand Risk Management Program Process

- Select program management controls
- Privacy requirements
- Determine third-party hosted information systems

### 1.3: Understand Regulatory and Legal Requirements

- Familiarize with governmental, organizational, and international regulatory security and privacy requirements (e.g., International Organization for Standardization (ISO) 27001, Federal Information Security Modernization Act (FISMA), Federal Risk and Authorization Management Program (FedRAMP), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA))
- Familiarize with other applicable security-related mandates

## Domain 2: Scope of the Information System (11%)

### 2.1: Define the Information System

- Determine the scope of the information system
- Describe the architecture (e.g., data flow, internal and external interconnections)
- Describe the information system's purpose and functionality

### 2.2: Determine Categorization of the Information System

- Identify the information types processed, stored, or transmitted by the information system
- Determine the impact level on confidentiality, integrity, and availability for each information type (e.g., Federal Information Processing Standards (FIPS) 199, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27002, data protection impact assessment)
- Determine information system categorization and document results

INFOSECTRAIN

## Domain 3: Selection and Approval of Security and Privacy Controls (15%)

### 3.1: Identify and Document Baseline and Inherited Controls

### 3.2: Select and Tailor Controls to the System

- Determine the applicability of recommended baseline and inherited controls
- Determine appropriate use of control enhancements (e.g., security practices, overlays, countermeasures)
- Document control applicability

### 3.3: Develop a Continuous Control Monitoring Strategy (e.g., Implementation, Timeline, Effectiveness)

### 3.4: Review and Approve Security Plan/Information Security Management System (ISMS)

INFOSECTRAIN

## Domain 4: Implementation of Security and Privacy Controls (16%)

### 4.1: Implement Selected Controls

- Determine mandatory configuration settings and verify implementation in accordance with current industry standards (e.g., Technical Security Standard for Information Technology (TSSIT), Technical Guideline for Minimum Security Measures, United States Government Configuration Baseline (USGCB), National Institute of Standards and Technology (NIST) checklists, Security Technical Implementation Guides (STIGs), Center for Internet Security (CIS) benchmarks, General Data Protection Regulation (GDPR))
- Ensure that the implementation of controls is consistent with the organizational architecture and associated security and privacy architecture
- Coordinate implementation of inherited controls with control providers

### 4.2: Document Control Implementation

- Document inputs to the planned controls, their expected behavior, and expected outputs or deviations
- Verify the documented details of the controls meet the purpose, scope, and risk profile of the information system
- Obtain and document implementation details from appropriate organization entities (e.g., physical security, personnel security, privacy)

INFOSECTRAIN

## Domain 5: Assessment/Audit of Security and Privacy Controls (16%)

### 5.1: Prepare for Assessment/Audit

- Determine assessor/auditor requirements
- Establish objectives and scope
- Determine methods and level of effort
- Determine necessary resources and logistics
- Collect and review artifacts (e.g., previous assessments/audits, system documentation, policies)
- Finalize the assessment/audit plan

### 5.2: Conduct Assessment/Audit

- Collect and document assessment/audit evidence
- Assess/audit implementation and validate compliance using approved assessment methods (e.g., interview, test, and examine)

### 5.3: Prepare the Initial Assessment/Audit Report

- Analyze assessment/audit results and identify vulnerabilities
- Propose remediation actions

### 5.4: Review the Initial Assessment/Audit Report and Perform Remediation

- Determine risk responses
- Apply remediations
- Reassess and validate the remediated controls

INFOSECTRAIN

### 5.5: Develop Final Assessment/Audit Report

### 5.6: Develop Remediation Plan

- Analyze identified residual vulnerabilities or deficiencies
- Prioritize responses based on risk level
- Identify resources (e.g., financial, personnel, and technical) and determine the appropriate time frame/schedule required to remediate deficiencies

## Domain 6: Authorization/Approval of Information Systems (10%)

### 6.1: Compile Security and Privacy Authorization/Approval Documents

- Compile required security and privacy documentation to support authorization/approval decisions by the designated official

### 6.2: Determine Information System Risk

- Evaluate information system risk
- Determine risk treatment options (i.e., accept, avoid, transfer, mitigate, share)
- Determine residual risk

### 6.3: Authorize/Approve Information System

- Determine terms of authorization/approval

INFOSECTRAIN

## Domain 7: Continuous Monitoring (16%)

### 7.1: Determine the Impact of Changes to the Information System and Environment

- Identify potential threats and impact on the operation of information systems and the environment
- Analyze risk due to proposed changes accounting for organizational risk tolerance
- Approve and document proposed changes (e.g., Change Control Board (CCB), Technical Review Board)
- Implement proposed changes
- Validate changes have been correctly implemented
- Ensure change management tasks are performed

### 7.2: Perform Ongoing Assessments/Audits Based on Organizational Requirements

- Monitor network, physical, and personnel activities (e.g., unauthorized assets, personnel, and related activities)
- Ensure vulnerability scanning activities are performed
- Review automated logs and alerts for anomalies (e.g., security orchestration, automation, and response)

### 7.3: Review Supply Chain Risk Analysis Monitoring Activities (e.g., Cyber Threat Reports, Agency Reports, News Reports)

INFOSECTRAIN

## 7.4: Actively Participate in Response Planning and Communication of a Cyber Event

- Ensure response activities are coordinated with internal and external stakeholders
- Update documentation, strategies, and tactics incorporating lessons learned

## 7.5: Revise Monitoring Strategies Based on Changes to Industry Developments Introduced Through Legal, Regulatory, Supplier, Securityand Privacy Updates

## 7.6: Keep Designated Officials Updated About the Risk Posture for Continuous Authorization/Approval

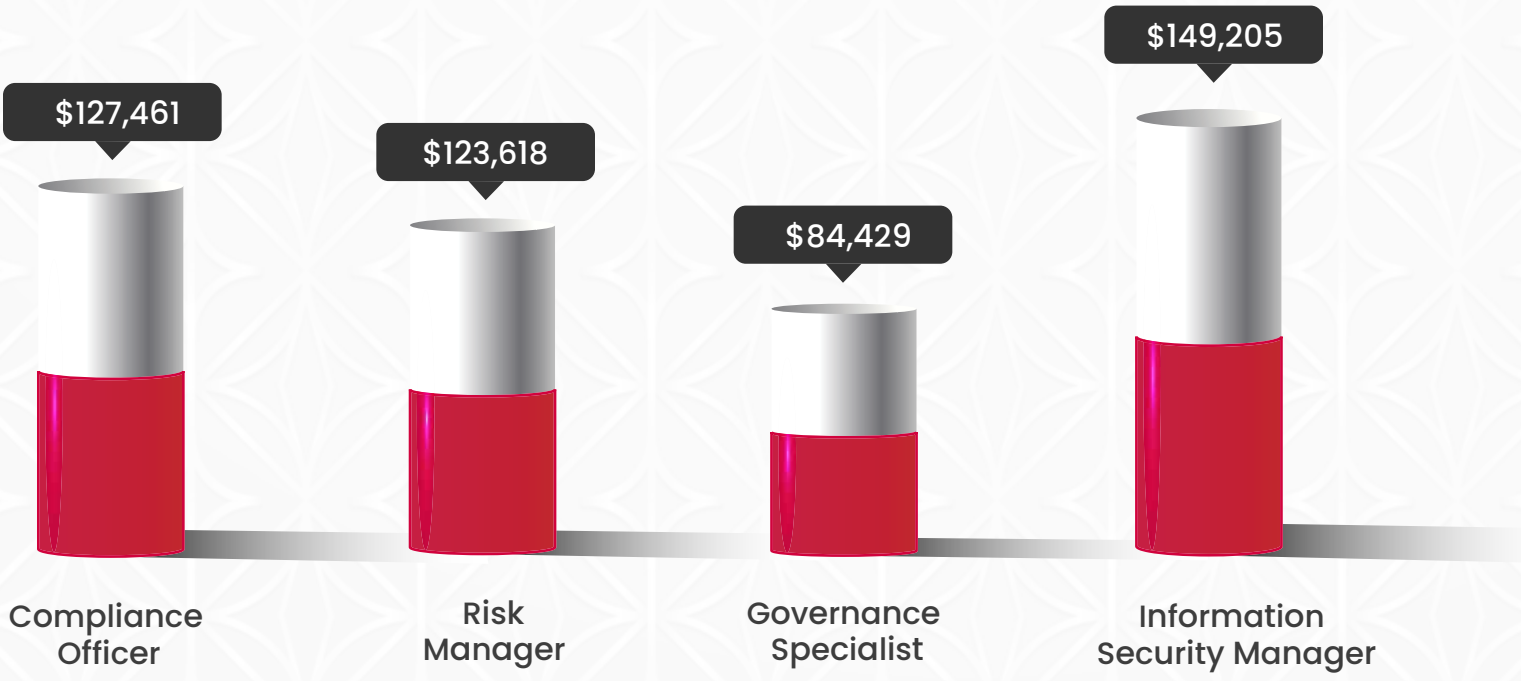
- Determine ongoing information system risk
- Update risk register, risk treatment, and remediation plan

## 7.7: Decommission Information System

- Determine information system decommissioning requirements
- Communicate decommissioning of information system
- Remove information system from operations

INFOSECTRAIN

# Course Benefits




## Hiring Companies

Google Deloitte. KPMG Microsoft

Source: Glassdoor, Indeed


www.infosectrain.com I sales@infosectrain.com