Document Generated: 11/15/2026

Learning Style: Online Instructor-Led

Technology: ISC2

Difficulty: Intermediate

Course Duration: 5 Days

ISC2 Certified in Governance, Risk and Compliance (CGRC)



The Certified in Governance, Risk and Compliance (CGRC) course, offered by (ISC)², is designed for professionals who manage and authorize information systems within a risk management framework. Formerly known as the Certified Authorization Professional (CAP), CGRC focuses on applying the NIST Risk Management Framework (RMF) to ensure the confidentiality, integrity, and availability of information systems.

Course Objectives:

- Purpose and importance of a risk management program
- Roles and responsibilities
- Risk tolerance and appetite
- Integrating security and risk management into system development lifecycle
- Regulatory and legal requirements
- Security categorization of information systems
- System boundaries and environment of operation
- Types of information processed, stored, or transmitted
- Impact levels (Confidentiality, Integrity, Availability)
- Baseline control selection (NIST SP 800-53)
- Tailoring and documenting controls
- Risk-based decision-making
- System-specific, common, and hybrid controls
- Implementing technical, administrative, and physical controls
- Configuration and deployment
- Documentation and evidence of control implementation
- Tools and technologies used in control implementation
- Assessment planning and preparation
- Conducting assessments (manual, automated, hybrid)
- Documenting assessment results
- Risk analysis and impact determination
- Risk determination and acceptance
- Developing the authorization package
- Communicating risks to authorizing officials

- Authorization decision and documentation
- Ongoing assessment of security and privacy controls
- Configuration management and change control
- Incident response and reporting
- Updates to risk management documentation
- Metrics and reporting for continuous improvement

Audience:

- Information Security Officers
- Risk and Compliance Managers
- IT Security Auditors
- Security Control Assessors

Prerequisites:

- At least two years of cumulative, paid work experience in one or more of the seven domains of the CGRC Common Body of Knowledge (CBK).
- A solid understanding of security and privacy frameworks such as NIST RMF, FISMA, and related compliance requirements is highly recommended.
- Candidates who do not yet meet the experience requirement can still take the exam and become an (ISC)² Associate, gaining full certification once they meet the work experience requirement.

Course Outline:

Domain 1: Information Security Risk Management Program

1.1 - Understand the foundation of an organization's 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 process

1.2 - Understand the 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

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 the 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

Domain 3: Selection and Approval of Security and Privacy Controls

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 continuous control monitoring strategy (e.g., implementation, timeline, effectiveness)

3.4 - Review and approve security plan/Information Security Management System (ISMS)

Domain 4: Implementation of Security and Privacy Controls

4.1 - Implement selected controls

- Determine mandatory configuration settings and verify implementation following 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
- Determine and implement compensating/alternate security controls

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)

Domain 5: Assessment/Audit of Security and Privacy Controls

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 actions

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

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 timeframe/schedule required to remediate deficiencies

Domain 6: Authorization/Approval of Information System

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

Domain 7: Continuous Monitoring

7.1 - Determine the impact of changes to information systems and the environment

- Identify potential threats and impacts to 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)

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, security and 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