The Computer Workshop
A Professional Development Company
614•798•9505 1•800•639•3535

Certified in Governance, Risk, and Compliance (CGRC)

Course ID #: 7000-797-ZZ-Z
Hours: 35

Course Content

Course Description:

This official (ISC)2® Certified in Governance, Risk and Compliance (CGRC) Training prepares you for the CGRC exam. The Certified Authorization Professional (CAP®) has changed its name to the Certified in Governance, Risk and Compliance (CGRC). This is only a title change, so the course modules, prerequisites, and delivery remain the same.

The Certified in Governance, Risk and Compliance (CGRC®) is an information security practitioner who advocates for security risk management in pursuit of information system authorization to support an organization's mission and operations in accordance with legal and regulatory requirements.

Passing the CAP Certification Exam meets U.S. DoD Directive 8140/8570.01 Management (IAM) Level-I and Management (IAM) Level-II requirements.

Course Objectives:

Upon successful completion of this course, students will be able to:

- Information Security Risk Management Program.
- Scope of the Information System.
- Selection and Approval of Security and Privacy Controls.
- Implementation of Security and Privacy Controls.
- Assessment/Audit of Security and Privacy Controls.
- Authorization/Approval of Information System.
- Perform Continuous Monitoring.

Prerequisites:

To qualify for the CGRC certification, you must have a minimum of two years of cumulative, paid, full-time work experience in one or more of the seven domains of the CGRC Common Body of Knowledge (CBK)

The Computer Workshop
A Professional Development Company
614•798•9505 1•800•639•3535

Certified in Governance, Risk, and Compliance (CGRC)

Course ID #: 7000-797-ZZ-Z
Hours: 35

Topics:

Information Security Risk Management Program

Lesson 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

Lesson 2: Understand risk management program processes

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

The Computer Workshop
A Professional Development Company
614•798•9505 1•800•639•3535

Certified in Governance, Risk, and Compliance (CGRC)

Course ID #: 7000-797-ZZ-Z

Hours: 35

Scope of the Information System

Lesson 3: Define the information system

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

Lesson 4: 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

Selection and Approval of Security and Privacy Controls

Lesson 5: Identify and document baseline and inherited controls 3.2 Select and tailor controls to the system

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

Lesson 6: Develop a continuous control monitoring strategy (e.g., implementation, timeline, effectiveness)

Lesson 7: Review and approve security plan/Information Security Management System (ISMS)

Implementation of Security and Privacy Controls

Lesson 8: Implement selected controls

- Determine mandatory configuration settings and verify implementation in accordance with current industry standards (e.g. appropriate organization entities (e.g., physical security, personnel security, privacy)

Assessment/Audit of Security and Privacy Controls

Lesson 9: 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

The Computer Workshop
A Professional Development Company
614•798•9505 1•800•639•3535

Certified in Governance, Risk, and Compliance (CGRC)

Course ID #: 7000-797-ZZ-Z

Hours: 35

Lesson 10: 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)

Lesson 11: Prepare the initial assessment/audit report

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

Lesson 12: Review initial assessment/audit report and perform remediation actions

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

Lesson 13: Develop final assessment/audit report

Lesson 14: Develop a 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

Authorization/Approval of Information System

Lesson 15: Compile security and privacy authorization/approval documents

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

Lesson 16: Determine information system risk

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

Lesson 17: Authorize/approve information system

- Determine terms of authorization/approval

Continuous Monitoring

Lesson 18: Determine the impact of changes to information systems and the environment

- Identify potential threats and impacts to the operation of information systems and environments
- 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

The Computer Workshop
A Professional Development Company
614•798•9505 1•800•639•3535

Certified in Governance, Risk, and Compliance (CGRC)

Course ID #: 7000-797-ZZ-Z
Hours: 35

Lesson 19: 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)

Lesson 20: Review supply chain risk analysis monitoring activities (e.g., cyber threat reports, agency reports, news reports)

Lesson 21: 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

Lesson 22: Revise monitoring strategies based on changes to industry developments introduced through legal, regulatory, supplier, security, and privacy updates

Lesson 23: 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

Lesson 24: Decommission information system

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