APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

ISC2 Certified in Governance, Risk and Compliance (CGRC) Training

Award Winning Training · Applied Technology Academy

The ISC2 Certified in Governance, Risk and Compliance credential — formerly known as the Certified Authorization Professional (CAP) — validates your understanding and skills within the field of GRC. It confirms that you know how to assess risk, establish security requirements, and create documentation using a broad range of security frameworks.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**5 Days**	**2 years: 1+ of the 7 domains**	**$124,610**	**Yes**

Course Overview

The broad spectrum of topics included in the CGRC Common Body of Knowledge (CBK®) ensure its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following seven domains:

- 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.

Course Outline

- **Domain 1: Information Security Risk Management Program**
  - 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 process

  - 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
- **Domain 2: Scope of the Information System**
  - 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
  - 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
- **Domain 3: Selection and Approval of Security and Privacy Controls**
  - Identify and document baseline and inherited controls
  - 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
  - Develop continuous control monitoring strategy (e.g., implementation, timeline, effectiveness)
  - Review and approve security plan/Information Security Management System (ISMS)
- **Domain 4: Implementation of Security and Privacy Controls**
  - Implement selected controls
  - Determine mandatory configuration settings and verify implementation in accordance with current industry standards (e.g., Information Technology Security Guidance ITSG-33 – Annex 3A, 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 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
  - 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**
  - 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
  - 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)
  - Prepare the initial assessment/audit report
  - Analyze assessment/audit results and identify vulnerabilities
  - Propose remediation actions
  - Review initial assessment/audit report and perform remediation actions
  - Determine risk responses
  - Apply remediations » Reassess and validate the remediated controls
  - Develop final assessment/audit report
  - 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**

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

  - Compile security and privacy authorization/approval documents
  - Compile required security and privacy documentation to support authorization/approval decision by the designated official
  - Determine information system risk
  - Evaluate information system risk
  - Determine risk treatment options (i.e., accept, avoid, transfer, mitigate, share)
  - Determine residual risk
  - Authorize/approve information system
  - Determine terms of authorization/approval
- **Domain 7: Continuous Monitoring**
  - Determine impact of changes to information system and environment
  - Identify potential threat and impact to operation of information system and 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
  - 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)
  - Review supply chain risk analysis monitoring activities (e.g., cyber threat reports, agency reports, news reports)
  - 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
  - Revise monitoring strategies based on changes to industry developments introduced through legal, regulatory, supplier, security, and privacy updates
  - 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
  - Decommission information system
  - Determine information system decommissioning requirements
  - Communicate decommissioning of information system
  - Remove information system from operations

Intended Audience

It is ideal for U.S. government officials who manage information system security for the Department of Defense (DoD), and it meets the requirements of DoD Directive 8140. Private-sector individuals who manage risk will also find the credential valuable because it shows a firm grasp of aligning business objectives with risk management and regulatory compliance.

A candidate that doesn't have the required experience to become a CGRC may become an Associate of $(ISC)^2$ by successfully passing the CGRC examination. The Associate of $(ISC)^2$ will then have three years to earn the two year required experience.

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).

CGRC Certification Information

To maintain certification, you must:

- Earn and post a minimum of 20 ISC2 CPE credits per year
- Comply with ISC2's Code of Professional Ethics

Follow-On Courses

ISACA Certified Risk and Information System Control (CRISC)

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.