Certified in Governance Risk and Compliance

Duration: 3 Days

Prerequisites:

Candidates must have a minimum of two years cumulative work experience in one or more of the seven domains of the CGRC CBK.
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.

Course Description:

Certified in Governance, Risk and Compliance (CGRCTM) cybersecurity professionals have the knowledge and skills to integrate governance, performance management, risk management and regulatory compliance within the organization while helping the organization achieve objectives, address uncertainty and act with integrity. CGRC professionals align IT goals with organizational objectives as they manage cyber risks and achieve regulatory needs. They utilize frameworks to integrate security and privacy with the organization's overall objectives, allowing stakeholders to make informed decisions regarding data security and privacy risks.

Course Outline:

Domain 1: Information Security Risk Management Program
- Understand the foundation of an organization information security risk management program
- Understand risk management program processes
- Understand regulatory and legal requirements

Domain 2: Scope of the Information System
- Define the information system
- Determine categorization of the information system

Domain 3: Selection and Approval of Security and Privacy Controls
- Identify and document baseline and inherited controls
- Select and tailor controls to the system
- Develop continuous control monitoring strategy
- Review and approve security plan/Information Security Management System (ISMS)

Domain 4: Implementation of Security and Privacy Controls
- Implement selected controls
- Document control implementation

Domain 5: Assessment/Audit of Security and Privacy Controls
- Prepare for assessment/audit
- Conduct assessment/audit
- Prepare the initial assessment/audit report
- Review initial assessment/audit report and perform remediation actions
- Develop final assessment/audit report
- Develop remediation plan

Domain 6: Authorization/Approval of Information System
- Compile security and privacy authorization/approval documents
- Determine information system risk
- Authorize/approve information system

Domain 7: Continuous Monitoring
- Determine impact of changes to information system and environment
- Perform ongoing assessments/audits based on organizational requirements
- 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
- 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
- Decommission information system