CGRC¬ Training and Certification

Course: **00058**
Filter: **Beginner**
Duration: **5 days**
Category:: **Cyber Security**
Price: **2500,00 €**

About Course

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 Certified in Governance, Risk and Compliance (CGRC). This is only a title change, so the course modules, prerequisites, and delivery remain the same. An individual certified in Governance, Risk and Compliance (CGRC) is an information security practitioner who advocates for security risk management in pursuit of information system authorization. This is needed to support an organization’s mission and operations in accordance with legal and regulatory requirements. Passing the CGRC Exam meets U.S. DoD Directive 8140/8570.01 Management (IAM) Level-I and Management (IAM) Level-II requirements.

What you'll learn

- 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.

Pre-requisites

- 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).

Curriculum

Module 1: Information Security Risk Management Program

- Understand the foundation of an organization's information security risk management program » Principles of information security
- Understand risk management program processes

Module 2: Scope of the Information System

- Define the information system
- Determine categorization of the information system

Module 3: Selection and Approval of Security and Privacy Controls

- Identify and document baseline and inherited controls
- Select and tailor controls to the system
- Develop a continuous control monitoring strategy (e.g., implementation, timeline, effectiveness)
- Review and approve security plan/Information Security Management System (ISMS)

Module 4: Implementation of Security and Privacy Controlsystem (ISMS)

- Implement selected controls

Module 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 a remediation plan

Module 6: Authorization/Approval of Information System

- Compile security and privacy authorization/approval documents
- Determine information system risk
- Authorize/approve information system

Module 7: Continuous Monitoring

- Determine the impact of changes to information systems and the 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