ISC2 Certified in Governance Risk and Compliance Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

This official (ISC)2® Certified in Governance, Risk and Compliance (CGRC) Training prepares you for the CGRC exam.

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

As an (ISC)2 Official Training Provider, we use courseware developed by (ISC) creator of the CGRC CBK to ensure your training is relevant and up-to-date. Our instructors are verified security experts who hold the CGRC and have completed intensive training to teach (ISC)² content.

Please Note: An Exam voucher is included with this course.

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).

What You Will Learn

In this CGRC Certification and Training, you will learn how to:

- Create an Information Security Risk Management Programme.
- 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.
- Authorisation/Approval of Information System.
- Perform Continuous Monitoring.

Training Outline

Domain 1: Information Security Risk Management Programme

1.1 Understand the foundation of an organisation's information security risk management programme » Principles of information security

BILGINC IT Academy

info@bilginc.com

bilginc.com

- Risk management frameworks (e.g., National Institute of Standards and Technology (NIST), cyber security framework, Control Objectives for Information and Related Technology (COBIT), International Organisation for Standardisation (ISO) 27001, International Organisation for Standardisation (ISO) 31000)
- System Development Life Cycle (SDLC)
- Information system boundary requirements
- Security controls and practices
- Roles and responsibilities in the authorisation/approval process

1.2 Understand risk management programme processes

- Select programme management controls
- Privacy requirements
- Determine third-party hosted information systems
- Understand regulatory and legal requirements
- Familiarise with governmental, organisational, and international regulatory security and privacy requirements (e.g., International Organisation for Standardisation (ISO) 27001, Federal Information Security Modernisation Act (FISMA), Federal Risk and Authorisation Management Programme (FedRAMP), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA))
- Familiarise 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 information system purpose and functionality

2.2 Determine categorisation 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 Organisation for Standardisation/ International Electrotechnical Commission (ISO/IEC) 27002, data protection impact assessment)
- Determine information system categorisation 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 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 a continuous control monitoring strategy (e.g., implementation, timeline, effectiveness)

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

BILGINC IT Academy

info@bilginc.com

bilginc.com

Domain 4: Implementation of Security and Privacy Controls

4.1 Implement selected controls

- Determine mandatory configuration settings and verify implementation in accordance with current industry standards (e.g. appropriate organisation 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 artefacts (e.g., previous assessments/audits, system documentation, policies)
- Finalise 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

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

5.4 Review 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 a remediation plan

- Analyse identified residual vulnerabilities or deficiencies
- Prioritise 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: Authorisation/Approval of Information System

6.1 Compile security and privacy authorisation/approval documents

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

6.2 Determine information system risk

- Evaluate information system risk

BILGINC IT Academy
info@bilginc.com
bilginc.com

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

6.3 Authorise/approve information system

- Determine terms of authorisation/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 environments
- Analyse risk due to proposed changes accounting for organisational 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 organisational requirements

- Monitor network, physical, and personnel activities (e.g., unauthorised 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 authorisation/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