CGRC™

Certified in Governance Risk and Compliance

An (ISC)² Certification

Certification **Exam Outline**

Effective Date: August 15, 2021

About CGRC

Certified in Governance, Risk and Compliance (CGRC™) 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.

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
- Continuous Monitoring

Experience Requirements

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. You can learn more about CGRC experience requirements and how to account for part-time work and internships at www.isc2.org/Certifications/CGRC/experience-requirements.

Accreditation

The certification is accredited by ANAB as being in compliance with the stringent requirements of ISO/IEC 17024:2012.

Job Task Analysis (JTA)

(ISC)² has an obligation to its membership to maintain the relevancy of the CGRC. Conducted at regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by security professionals who are engaged in the profession defined by the CGRC. The results of the JTA are used to update the examination. This process ensures that candidates are tested on the topic areas relevant to the roles and responsibilities of today's practicing information security professionals.

CGRC Examination Information

Length of exam	3 hours
Number of items	125
Item format	Multiple choice
Passing grade	700 out of 1000 points
Exam availability	English
Testing center	Pearson VUE Testing Center

CGRC Examination Weights

Domains	Weight
1. Information Security Risk Management Program	16%
2. Scope of the Information System	11%
3. Selection and Approval of Security and Privacy Controls	15%
4. Implementation of Security and Privacy Controls	16%
5. Assessment/Audit of Security and Privacy Controls	16%
6. Authorization/Approval of Information System	10%
7. Continuous Monitoring	16%
Total:	**100%**

Domain 1: Information Security Risk Management Program

1.1 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

1.2 Understand risk management program processes

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

1.3 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

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 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

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 continuous control monitoring strategy (e.g., implementation, timeline, effectiveness)

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

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., 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

4.2 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

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 artifacts (e.g., previous assessments/audits, system documentation, policies)
- Finalize 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

- Analyze 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 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

6.1 Compile security and privacy authorization/approval documents

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

6.2 Determine information system risk

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

6.3 Authorize/approve information system

» Determine terms of authorization/approval

Domain 7: Continuous Monitoring

7.1 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

7.2 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)

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 authorization/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

Additional Examination Information

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the CBK and identifying areas of study that may need additional attention.

View the full list of supplementary references at www.isc2.org/certifications/References.

Examination Policies and Procedures

(ISC)² recommends that CGRC candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at www.isc2.org/Register-for-Exam.

Legal Information

For any questions related to (ISC)²'s legal policies, please contact the (ISC)² Legal Department at legal@isc2.org.

Any Questions?

Contact (ISC)² Candidate Services in your region:

Americas
Phone: +1-866-331-ISC2 (4722)
Email: info@isc2.org

Asia Pacific
Phone: +852-5803-5662
Email: isc2asia@isc2.org

Europe, Middle East and Africa
Phone: +44-203-960-7800
Email: info-emea@isc2.org