ISC2 CGRC

ISC2 Governance, Risk and Compliance Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

CGRC

ISC2 Certified Governance, Risk and Compliance

125 Questions Exam – 700 / 1000 Cut Score – Duration of 180 minutes




EDUSUM

#1 Online Certification Guide

Table of Contents:

Discover More about the CGRC Certification

Are you interested in passing the ISC2 CGRC exam? First discover, who benefits from the CGRC certification. The CGRC is suitable for a candidate if he wants to learn about Security Assessment and Authorization. Passing the CGRC exam earns you the ISC2 Certified Governance, Risk and Compliance title.

While preparing for the CGRC exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The CGRC PDF contains some of the most valuable preparation tips and the details and instant access to useful **CGRC study materials just at one click.**

ISC2 CGRC ISC2 Governance, Risk and Compliance Certification Details:

Exam Name	ISC2 Certified Governance, Risk and Compliance (CGRC)
Exam Code	CGRC
Exam Price	$599 (USD)
Duration	180 mins
Number of Questions	125
Passing Score	700 / 1000
Schedule Exam	**Pearson VUE**
Sample Questions	**ISC2 CGRC Sample Questions**
Practice Exam	**ISC2 CGRC Certification Practice Exam**

CGRC Syllabus:

Topic	Details
Information Security Risk Management Program - 16%	
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

Topic	Details
	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
Scope of the Information System - 11%	
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)

Topic	Details
	- Determine information system categorization and document results
Selection and Approval of Security and Privacy Controls - 15%	
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)	
Implementation of Security and Privacy Controls - 16%	
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

Topic	Details
	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)
Assessment/Audit of Security and Privacy Controls - 16%	
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

Topic	Details
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
Authorization/Approval of Information System - 10%	
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
Continuous Monitoring - 16%	
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	- Monitor network, physical and personnel activities (e.g., unauthorized assets, personnel and related activities)

Topic	Details
based on organizational requirements	- 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

Broaden Your Knowledge with ISC2 CGRC Sample Questions:

Question: 1

When an authorizing official (AO) submits the security authorization decision, what responses should the information system owner (ISO) expect to receive?

a) Authorized to operate (ATO) or denial authorization to operate (DATO), the conditions for the authorization placed on the information system and owner, and the authorization termination date
b) Authorized to Operate (ATO) or Denial Authorization to Operate (DATO), the list of security controls accessed, and an system contingency plan
c) Authorized to operate (ATO) or denial authorization to operate (DATO), and the conditions for the authorization placed on the information system and owner
d) A plan of action and milestones (POA&M), the conditions for the authorization placed on the information system and owner, and the authorization termination date

Answer: a

Question: 2

Which authorization approach considers time elapsed since the authorization results were produced, the environment of operation, the criticality/sensitivity of the information, and the risk tolerance of the other organization?

a) Leveraged
b) Single
c) Joint
d) Site specific

Answer: a

Question: 3

What key information is used by the authorizing official (AO) to assist with the risk determination of an information system (IS)?

a) Security authorization package (SAP)
b) Plan of action and milestones (POA&M)
c) Security plan (SP)
d) Interconnection security agreement (ISA)

Answer: a

Question: 4

Documenting the description of the system in the system security plan is the primary responsibility of which Risk Management Framework (RMF) role?

a) Authorizing official (AO)
b) Information owner
c) Information system security officer (ISSO)
d) Information system owner

Answer: d

Question: 5

Information developed from Federal Information Processing Standard (FIPS) 199 may be used as an input to which authorization package document?

a) Security assessment report (SAR)
b) System security plan (SSP)
c) Plan of actions and milestones (POA&M)
d) Authorization decision document

Answer: b

Question: 6

Who determines the required level of independence for security control assessors?

a) Information system owner (ISO)
b) Information system security manager (ISSM)
c) Authorizing official (AO)
d) Information system security officer (ISSO)

Answer: c

Question: 7

System authorization is now used to refer to which of the following terms?

a) System security declaration
b) Certification and accreditation
c) Security test and evaluation
d) Continuous monitoring

Answer: b

Question: 8

According to the Risk Management Framework (RMF), which role has a primary responsibility to report the security status of the information system to the authorizing official (AO) and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy?

a) Information system security officer (ISSO)
b) Common control provider
c) Independent assessor
d) Senior information assurance officer (SIAO)

Answer: b

Question: 9

Why is security control volatility an important consideration in the development of a security control monitoring strategy?

a) It identifies needed security control monitoring exceptions.
b) It indicates a need for compensating controls.
c) It establishes priority for security control monitoring.
d) It provides justification for revisions to the configuration management and control plan.

Answer: c

Question: 10

When should the information system owner document the information system and authorization boundary description in the security plan?

a) After security controls are implemented
b) While assembling the authorization package
c) After security categorization
d) When reviewing the security control assessment plan

Answer: c

Avail the Study Guide to Pass ISC2 CGRC ISC2 Governance, Risk and Compliance Exam:

- Find out about the CGRC syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **CGRC syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the CGRC training. Joining the ISC2 provided training for CGRC exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **CGRC sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. CGRC practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the CGRC exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.

Here Is the Trusted Practice Test for the CGRC Certification

EduSum.Com is here with all the necessary details regarding the CGRC exam. We provide authentic practice tests for the CGRC exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on EduSum.Com for rigorous, unlimited two-month attempts on the **CGRC practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the ISC2 Certified Governance, Risk and Compliance.

Start Online practice of CGRC Exam by visiting URL
https://www.edusum.com/isc2/cgrc-isc2-governance-risk-and-compliance