Certified in Governance Risk and Compliance

ISC2 Certification

Certification **Exam Outline**

Effective Date: June 15, 2024

ISC2

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 domains:

- Security and Privacy Governance, Risk Management, and Compliance Program
- Scope of the System
- Selection and Approval of Framework, Security, and Privacy Controls
- Implementation of Security and Privacy Controls
- Assessment/Audit of Security and Privacy Controls
- System Compliance
- Compliance Maintenance

Experience Requirements

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

A candidate that doesn't have the required experience to become a CGRC may become an Associate of ISC2 by successfully passing the CGRC examination. The Associate of ISC2 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)

ISC2 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. Security and Privacy Governance, Risk Management, and Compliance Program	16%
2. Scope of the System	10%
3. Selection and Approval of Framework, Security, and Privacy Controls	14%
4. Implementation of Security and Privacy Controls	17%
5. Assessment/Audit of Security and Privacy Controls	16%
6. System Compliance	14%
7. Compliance Maintenance	13%
Total:	**100%**

Domain 1: Security and Privacy Governance, Risk Management, and Compliance Program

1.1 Demonstrate knowledge in security and privacy governance, risk management, and compliance program

- Principles of governance, risk management, and compliance
- Risk management and compliance frameworks using national and international standards and guidelines for security and privacy requirements (e.g., National Institute of Standards and Technology (NIST), cybersecurity framework, Control Objectives for Information and Related Technology (COBIT), International Organization for Standardization/International Electrotechnical Commission (ISO/IEC))
- System Development Life Cycle (SDLC) (e.g., requirements gathering, design, development, testing, and operations/maintenance/disposal)
- Information lifecycle for each data type processed, stored, or transmitted (e.g., retaining, disposal/destruction, data flow, marking)
- Confidentiality, integrity, availability, non-repudiation, and privacy concepts
- System assets and boundary descriptions
- Security and privacy controls and requirements
- Roles and responsibilities for compliance activities and associated frameworks

1.2 Demonstrate knowledge in security and privacy governance, risk management and compliance program processes

- Establishment of compliance program for the applicable framework

1.3 Demonstrate knowledge of compliance frameworks, regulations, privacy, and security requirements

- Familiarity with compliance frameworks (e.g., International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), Federal Risk and Authorization Management Program (FedRAMP), Payment Card Industry Data Security Standard (PCI-DSS), Cybersecurity Maturity Model Certification)
- Familiarity with other national and international laws and requirements for security and privacy (e.g., Federal Information Security Modernization Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), executive orders, General Data Protection Regulation (GDPR))

Domain 2: Scope of the System

2.1 Describe the system

» System name and scope documented

» System purpose and functionality

2.2 Determine security compliance required

» Information types processed, stored, or transmitted

» Security objectives outlined for each information type based on national and international security and privacy compliance requirements (e.g., Federal Information Processing Standards (FIPS), International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), data protection impact assessment)

» Risk impact level determined for system based on the selected framework

Domain 3:
Selection and Approval of Framework, Security, and Privacy Controls

3.1 Identify and document baseline and inherited controls

3.2 Select and tailor controls

- Determination of applicable baseline and/or inherited controls
- Determination of appropriate control enhancements (e.g., security practices, overlays, mitigating controls)
- Specific data handling/marking requirements identified
- Control selection documentation
- Continued compliance strategy (e.g., continuous monitoring, vulnerability management)
- Control allocation and stakeholder agreement

Domain 4:
Implementation of Security and Privacy Controls

4.1 Develop implementation strategy (e.g., resourcing, funding, timeline, effectiveness)

- Control implementation aligned with organizational expectations, national or international requirements, and compliance for security and privacy controls
- Identification of control types (e.g., management, technical, common, operational control)
- Frequency established for compliance documentation reviews and training

4.2 Implement selected controls

- Control implementation consistent with compliance requirements
- Compensating or alternate security controls implemented

Domain 5:
Assessment/Audit of Security and Privacy Controls

5.1 Prepare for assessment/audit

- Stakeholder roles and responsibilities established
- Objectives, scope, resources, schedule, deliverables, and logistics outlined
- Assets, methods, and level of effort scoped
- Evidence for demonstration of compliance audited (e.g., previous assessments/audits, system documentation, policies)
- Assessment/audit plan finalized

5.2 Conduct assessment/audit

- Compliance capabilities verified using appropriate assessment methods: interview, examine, test (e.g., penetration, control, vulnerability scanning)
- Evidence verified and validated

5.3 Prepare the initial assessment/audit report

- Risks identified during the assessment/audit provided
- Risk mitigation summaries outlined
- Preliminary findings recorded

5.4 Review initial assessment/audit report and plan risk response actions

- Risk response assigned (e.g., avoid, accept, share, mitigate, transfer) based on identified vulnerabilities or deficiencies
- Risk response collaborated with stakeholders
- Non-compliant findings with newly applied corrective actions reassessed and validated

5.5 Develop final assessment/audit report

- Final compliance documented (e.g., compliant, non-compliant, not applicable)
- Recommendations documented when appropriate
- Assessment report finalized

5.6 Develop risk response plan

- Residual risks and deficiencies identified
- Risk prioritized
- Required resources identified (e.g., financial, personnel, and technical) to determine time required to mitigate risk

Domain 6: System Compliance

6.1 Review and submit security/privacy documents

» Security and privacy documentation required to support a compliance decision by the appropriate party (e.g., authorizing official, third-party assessment organizations, agency) compiled, reviewed, and submitted

6.2 Determine system risk posture

» System risk acceptance criteria
» Residual risk determination
» Stakeholder concurrence for risk treatment options
» Residual risks defined in formal documentation

6.3 Document system compliance

» Formal notification of compliance decision
» Formal notification shared with stakeholders

Domain 7: Compliance Maintenance

7.1 Perform system change management

» Changes weigh the impact to organizational risk, operations, and/or compliance requirements (e.g., revisions to baselines)

» Proposed changes documented and approved by authorized personnel (e.g., Change Control Board (CCB), technical review board)

» Deploy to the environment (e.g., test, development, production) with rollback plan

» Changes to the system tracked and compliance enforced

7.2 Perform ongoing compliance activities based on requirements

» Frequency established for ongoing compliance activities review with stakeholders)

» System and assets monitored (e.g., physical and logical assets, personnel, change control)

» Incident response and contingency activities performed)

» Security updates performed and risks remediated/tracked

» Evidence collected, testing performed, documentation updated (e.g., service level agreements, third party contracts, policies, procedures), and submission/communication to stakeholders when applicable

» Awareness and training performed, documented, and retained (e.g., contingency, incident response, annual security and privacy)

» Revising monitoring strategies based on updates to legal, regulatory, supplier, security and privacy requirements

7.3 Engage in audits activities based on compliance requirements

» Required testing and vulnerability scanning performed

» Personnel interviews conducted

» Documentation reviewed and updated

7.4 Decommission system when applicable

» Requirements for system decommissioning reviewed with stakeholders

» System removed from operations and decommissioned

» Documentation of the decommissioned system retained and shared with stakeholders

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

ISC2 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 ISC2's legal policies, please contact the ISC2 Legal Department at legal@ISC2.org.

Any Questions?

Contact ISC2 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

ISC2