Training: ISC2
ISC2 CGRC Certification Prep Course

TRAINING GOALS:

Official ISC2 CBK Training Seminar for the CGRC (Certified in Governance, Risk and Compliance)

The Official ISC2 Certified in Governance, Risk and Compliance (CGRC) Training Seminar provides a comprehensive review of information systems security concepts and industry best practices, covering the seven domains of the CGRC Common Body of Knowledge (CBK):

- Domain 1: Information Security Risk Management Program
- Domain 2: Scope of the Information System
- Domain 3: Selection and Approval of Security and Privacy Controls
- Domain 4: Implementation of Security and Privacy Controls
- Domain 5: Assessment/Audit of Security and Privacy Controls
- Domain 6: Authorization/Approval of Information System
- Domain 7: Continuous Monitoring

*Each participant in an authorized training **ISC2 CGRC Certification Prep Course** held in Compendium CE will receive a free CGRC Certification Exam voucher.*

This training course is structured around the steps of the NIST Risk Management Framework version 2.0, as covered in NIST Special Publication 800-37 Revision 2. The previous version, Revision 1, will be covered throughout the course as it corresponds to the current revision. This course will help students review and refresh their information security knowledge as they pursue the CGRC certification.

Course objectives

At the end of this course, learners will be able to:

- Identify and describe the steps and tasks within the NIST Risk Management Framework (RMF).
- Apply common elements of other risk management frameworks using the RMF as a guide.
- Describe the roles associated with the RMF and how they are assigned to tasks within the RMF.
- Execute tasks within the RMF process based on assignment to one or more RMF roles.
- Explain organizational risk management and how it is supported by the RMF.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

Intended audience

This course is for individuals planning to pursue the CGRC certification. The CGRC is ideal for IT, information security and information assurance practitioners and contractors who use the RMF in federal government, military, civilian roles, local governments and private sector organizations. Roles include:

- ISSOs, ISSMs and other infosec/information assurance practitioners who are focused on security assessment and authorization (traditional C&A) and continuous monitoring issues.
- Executives who must "sign off" on Authority to Operate (ATO).
- Inspector generals (IGs) and auditors who perform independent reviews.
- Program managers who develop or maintain IT systems.
- IT professionals interested in improving cybersecurity and learning more about the importance of lifecycle cybersecurity risk management.

Prior to taking this course the learner should have the following experience, skills, or knowledge in:

- IT security
- Information assurance
- Information risk management
- Certification
- Systems administration
- One to two years of general technical experience
- Two years of general systems experience
- One to two years of database/systems development/network experience
- Information security policy
- Technical or auditing experience within government, the U.S. Department of Defense, the financial or health care industries, and/or auditing firms
- Strong familiarity with NIST documentation

CONSPECT:

- Prepare
  - Explain the purpose and value of preparation.
  - Identify references associated with the Prepare step.
  - Identify other risk management frameworks and their relationship to RMF tasks.
  - Identify relevant security and privacy regulations.
  - List the references, processes and outcomes that define:
  - RMF Task P-1: Risk Management Roles

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- RMF Task P-2: Risk Management Strategy
- RMF Task P-3: Risk Assessment – Organization
- RMF Task P-14: Risk Assessment – System
- RMF Task P-4: Organizationally Tailored Control Baselines and Cybersecurity Framework Profiles
- RMF Task P-5: Common Control Identification
- RMF Task P-6: Impact-Level Prioritization
- RMF Task P-7: Continuous Monitoring Strategy – Organization
- RMF Task P-8: Mission or Business Focus
- RMF Task P-9: System Stakeholders
- RMF Task P-10: Asset Identification
- RMF Task P-11: Authorization Boundary
- RMF Task P-12: Information Types
- RMF Task P-13: Information Life Cycle
- RMF Task P-15: Requirements Definition
- RMF Task P-16: Enterprise Architecture
- RMF Task P-17: Requirements Allocation
- RMF Task P-18: System Registration
- Complete selected Prepare Tasks for the example system.

- Categorize
  - Explain the purpose and value of categorization.
  - Identify references associated with the Categorize step.
  - List the references, processes, and outcomes that define Risk Management Framework (RMF) Task C-1: System Description.
  - Describe a system’s architecture.
  - Describe an information system’s purpose and functionality.
  - Describe and document a system’s characteristics.
  - List the references, processes and outcomes that define RMF Task C-2: Security Categorization.
  - Categorize an information system.
  - List the references, processes and outcomes that define RMF Task C-3: Security Categorization Review and Approval.
  - Describe the review and approval process for security categorization.
  - Categorize the example systems.
- Select
  - Explain the purpose and value of control selection and allocation.
  - Identify references associated with the Select step.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Relate the ISO 27001 Statement of Applicability to the NIST RMF.
- List the references, processes and outcomes that define RMF Task S-1: Control Selection.
- List the references, processes and outcomes that define RMF Task S-2: Control Tailoring.
- Select appropriate security control baselines based on organizational guidance.
- Tailor controls for a system within a specified operational environment.
- List the references, processes and outcomes that define RMF Task S-3: Control Allocation.
- List the references, processes and outcomes that define RMF Task S-4: Documentation of Planned Control Implementations.
- Allocate security and privacy controls to the system and to the environment of operation.
- Document the controls for the system and environment of operation in security and privacy plans.
- List the references, processes and outcomes that define RMF Task S-5: Continuous Monitoring Strategy - System.
- Develop and implement a system-level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy.
- List the references, processes and outcomes that define RMF Task S-6: Plan Review and Approval.
- Review and approve the security and privacy plans for the system and the environment of operation.
- Allocate security controls for the example system.
- Tailor security controls for the example system.
- Draft a continuous monitoring plan for the example system.

- Implement
  - Explain the purpose and value of implementation.
  - Identify references associated with the Implement step.
  - List the references, processes and outcomes that define RMF Task I-1: Control Implementation.
  - Identify appropriate implementation guidance for control frameworks.
  - Integrate privacy requirements with system implementation.
  - List the references, processes and outcomes that define RMF Task I-2: Update Control Implementation Information.
  - Update a continuous monitoring strategy.
  - Update a control implementation plan.
- Assess
  - Explain the purpose and value of assessment.
  - Identify references associated with the Assess step.
  - Understand and identify common elements of the NIST process that are included in other frameworks and processes.
  - List the references, processes and outcomes that define RMF Task A-1: Assessor

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

Selection.

- List the references, processes and outcomes that define RMF Task A-2: Assessment Plan.
- List the references, processes and outcomes that define RMF Task A-3: Control Assessment.
- List the references, processes and outcomes that define RMF Task A-4: Assessment Reports.
- List the references, processes and outcomes that define RMF Task A-5: Remediation Actions.
- List the references, processes and outcomes that define RMF Task A-6: Plan of Action and Milestones.
- Develop an assessment plan for identified controls in the example system.
- Develop a remediation plan for unsatisfied controls in the example system.

- Authorize
  - Explain the purpose and value of authorization.
  - Identify references associated with the Authorize step.
  - Relate system approvals under organizational processes to the concepts applied in the NIST RMF.
  - List the references, processes and outcomes that define RMF Task R-1: Authorization Package.
  - List the references, processes and outcomes that define RMF Task R-2: Risk Analysis and Determination.
  - List the references, processes and outcomes that define RMF Task R-3: Risk Response.
  - List the references, processes and outcomes that define RMF Task R-4: Authorization Decision.
  - List the references, processes and outcomes that define RMF Task R-5: Authorization Reporting.
  - Develop a risk determination for the example system on the system risk level.
  - Authorize the system for operation.
  - Determine appropriate elements for the Authorization decision document for the example system.
- Monitor
  - Explain the purpose and value of monitoring.
  - Identify references associated with the Monitor step.
  - List the references, processes and outcomes that define RMF Task M-1: System and Environment Changes.
  - (Coordinate) Integrate cybersecurity risk management with organizational change management.
  - List the references, processes and outcomes that define RMF Task M-2: Ongoing Assessments.
  - Monitor risks associated with supply chain.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- List the references, processes and outcomes that define RMF Task M-3: Ongoing Risk Response.
- Understand elements for communication surrounding a cyber event.
- List the references, processes and outcomes that define RMF Task M-4: Authorization Package Updates.
- List the references, processes and outcomes that define RMF Task M-5: Security and Privacy Reporting.
- List the references, processes and outcomes that define RMF Task M-6: Ongoing Authorization.
- List the references, processes and outcomes that define RMF Task M-7: System Disposal.
- Discuss Monitor step activities in the example system.

- CGRC Certification Information
  - This chapter covers important information about the experience requirements for the Certified in Governance, Risk and Compliance (CGRC) certification and ISC2 exam policies and procedures. Details were based on information as of August 2021. It is recommended that learners go to the ISC2 website www.isc2.org for the most up-to-date information on certification requirements and the exam process.

REQUIREMENTS:

To qualify for the CGRC you must have a minimum of two years of cumulative paid work experience in one or more of the seven domains of the CGRC Common Body of Knowledge (CBK).

If you do not have the required experience to earn the CGRC, you may become an Associate of ISC2 by successfully passing the CGRC examination. As an Associate of ISC2, you will then have three years to earn the two years of required, relevant experience.

Part-time work and internships may also count towards your experience.

Valid experience includes information systems security-related work performed in pursuit of information system authorization, or work that requires security risk management knowledge and involves direct application of that knowledge. Experience must fall within one or more of the seven domains of the ISC2 CGRC CBK:

- Domain 1: Information Security Risk Management Program
- Domain 2: Scope of the Information System
- Domain 3: Selection and Approval of Security and Privacy Controls
- Domain 4: Implementation of Security and Privacy Controls
- Domain 5: Assessment/Audit of Security and Privacy Controls
- Domain 6: Authorization/Approval of Information System
- Domain 7: Continuous Monitoring

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

More information https://www.isc2.org/Certifications/CGRC/Experience-Requirements

Difficulty level

CERTIFICATE:

The participants will obtain certificates signed by ISC2 (course completion).

In order to complete the course, receive a certificate of completion and earn ISC2 continuing professional education (CPE) credits learners must:

- Complete all learning activities within the course.
- Complete a course evaluation.
- Score 70% or higher on end of chapter quizzes and final assessment.

An electronic Certificate of Completion will be provided once you have completed the course by meeting all the requirements. We recommend that you download and retain the certificate of completion as proof of credits earned.

This course will help prepare you also for the CGRC certification exam available at Pearson VUE test centers.

*Each participant in an authorized training **ISC2 CGRC Certification Prep Course** held in Compendium CE will receive a free CGRC Certification Exam voucher.*

TRAINER:

ISC2 Authorized Instructor

ADDITIONAL INFORMATION:

Participating in this training you get 40 CPE (Continuing Professional Education) credits.

CPE credits for ISC2 credentials must be self-reported by members and associates through the ISC2 CPE Portal accessible via www.isc2.org using your member login credentials.

CPE credits earned for this course may be eligible for continuing professional education credits for non-ISC2 certifications. Please visit the continuing education requirements established by the credentialing organization for eligibility.

For specific questions related to your CPE credits or the CPE portal please contact member support - membersupport@isc2.org.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007