Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com
Phone: +46 8 555 188 00

CGRC - Certified in Governance, Risk and Compliance

CODE:	LENGTH:	PRICE:
ISC_CGRC	280 Hours (35 days)	kr28,000.00

Description

Official ISC2 CBK Training for the CGRC

Official ISC2® Training Seminar for the Certified in Governance, Risk and Compliance (CGRC TM) provides a comprehensive review of the knowledge required for authorizing and maintaining information systems within the NIST Risk Management Framework. This training course will help students review and refresh their knowledge and identify areas they need to study for the CGRC exam. Content aligns with and comprehensively covers the seven domains of the ISC2 CGRC Common Body of Knowledge (CBK®).

Official courseware is developed by ISC2 – 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 ISC2 content.

Training features:

- Instruction from an ISC2 Authorized Instructor
- Official ISC2 Student Training Guide
- Chapter quizzes
- Interactive flash cards to reinforce learning
- 9 example system exercises teaching you how apply the steps of the Risk Management Framework (RMF).
- 13 discussions encouraging peer to peer interaction around key topics
- 7 end of chapter quizzes with answer explanation to assess comprehension
- 142 question post course assessment with answer explanation highlighting areas for further study

Course Domains

- 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

Objectives

After completing this course, the student 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.

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.

Programme

Domains/Modules/Chapters
This course covers the following chapters and learning objectives:

Chapter 1: Prepare (10 Modules)

- 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
    - 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.

Chapter 2: Categorize (5 Modules)

- 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.

Chapter 3: Select (7 Modules)

- Explain the purpose and value of control selection and allocation.
- Identify references associated with the Select step.
- 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.

Chapter 4: Implement (5 Modules)

- 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.

Chapter 5: Assess (6 Modules)

- 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 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.

Chapter 6: Authorize (6 Modules)

- 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.

Chapter 7: Monitor (8 Modules)

- 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.
- 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.

Chapter 8: CGRC Certification Information
This chapter covers important information about the experience requirements for the Certified Authorization Professional (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.

Note: Throughout this course, exam domains may be covered in several chapters. Included in the course is a table indicating where the exam outline

Session Dates

På begäran, kontakta oss

Ytterligare information

Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.