COURSE SYLLABUS

CGRC Exam Preparation Course (Self-Paced)

Learn the seven CGRC domains for taking a system from risk categorization through authorization and monitoring.

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/cgrc-exam-preparation-course-self-paced

support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1: Foundations of Information Security Risk Management

- Lessons:
  - What risk management means for an information system
  - The risk management life cycle: from NIST SP 800-37 to the CGRC's seven domains
  - Federal and commercial risk management compared
- Applied activity: Learners map a provided case-study organization's risk decisions to the seven-step life cycle and identify which step is weakest.

Module 2: Risk Management Roles, Governance and Legal Authorities

- Lessons:
  - Core roles: authorizing official, ISSO, system owner and risk executive
  - Governance structures that oversee the program
  - Legal and policy authorities behind federal risk management, and their commercial equivalents
- Applied activity: Learners sort ten responsibilities into the correct role and justify one placement in writing.

Module 3: Aligning the Risk Management Program with Organizational Risk Tolerance

- Lessons:
  - Defining organizational risk tolerance and risk appetite
  - Building a risk management strategy that reflects tolerance
  - Communicating risk tolerance decisions to system-level teams
- Applied activity: Learners draft a short risk tolerance statement for a fictional organization and explain how it would change one downstream control decision.

Module 4: Defining the System and Its Authorization Boundary

- Lessons:

- What counts as a system for authorization purposes
- Drawing the authorization boundary
- Common boundary-scoping mistakes

- Applied activity: Given a network diagram, learners draw the authorization boundary and justify what is included or excluded.

Module 5: Categorizing Information and Information Systems

- Lessons:
  - Information types and impact levels
  - Applying FIPS 199 categorization to confidentiality, integrity and availability
  - Documenting the categorization decision
- Applied activity: Learners categorize a public-facing website and a payroll system and defend their impact ratings.

Module 6: Registering the System and Assigning Security Responsibilities

- Lessons:
  - System registration and inventory requirements
  - Assigning the system owner, ISSO and other security roles
  - Linking scoping decisions to the system security plan
- Applied activity: Learners complete a short system registration form for a case-study system, assigning roles and citing its categorization.

Module 7: Control Baselines and Tailoring

- Lessons:
  - Control families and baselines in NIST SP 800-53
  - Tailoring a baseline to a system's actual risk
  - Documenting tailoring decisions
- Applied activity: Learners select a baseline for a moderate-impact case-study system and tailor two controls, documenting the rationale.

Module 8: Selecting Privacy Controls and Overlays

- Lessons:
  - Privacy controls and their relationship to security controls
  - Applying overlays for specialized environments
  - Coordinating privacy and security control selection
- Applied activity: Learners identify which privacy controls apply to a system that processes personally identifiable information and select an overlay.

Module 9: Documenting Controls in the System Security Plan

- Lessons:
  - Purpose and structure of the system security plan
  - Writing defensible control implementation statements
  - Review and approval of the security plan
- Applied activity: Learners write one implementation statement for a selected control and self-review it against a provided checklist.

Module 10: Translating the Security Plan into Implemented Controls

- Lessons:
  - From plan to practice: implementation planning
  - Sequencing implementation by risk priority
  - Common implementation gaps

- Applied activity: Learners build a short implementation checklist for one technical and one administrative control.

Module 11: Common Controls, Inheritance and Shared Responsibility

- Lessons:
  - Common controls and control inheritance
  - Shared responsibility in cloud and multi-tenant environments
  - Documenting inherited controls
- Applied activity: Given a cloud provider's responsibility matrix, learners identify which controls the system owner must still implement.

Module 12: Recording Implementation Evidence

- Lessons:
  - What counts as implementation evidence
  - Organizing evidence for later assessment
  - Avoiding evidence gaps before assessment begins
- Applied activity: Learners assemble a short evidence package for one implemented control from a case study.

Module 13: Building the Security Assessment Plan

- Lessons:
  - Purpose and components of a security assessment plan
  - Scoping the assessment to the system boundary
  - Selecting assessment procedures from NIST SP 800-53A
- Applied activity: Learners draft a one-page assessment plan outline for two controls from the case-study security plan.

Module 14: Assessment Methods: Examine, Interview and Test

- Lessons:
  - The examine method
  - The interview method
  - The test method
- Applied activity: Learners choose the correct assessment method for each of five sample controls and explain why.

Module 15: Analyzing Assessment Results and Identifying Weaknesses

- Lessons:
  - Rating assessment results
  - Distinguishing a weakness from a deficiency
  - Root-cause analysis of a finding
- Applied activity: Given three assessment findings, learners rate severity and identify the likely root cause of each.

Module 16: Reporting Findings in the Security Assessment Report

- Lessons:
  - Structure of the security assessment report
  - Writing findings that support a risk decision
  - Delivering the report to the system owner and authorizing official
- Applied activity: Learners write one finding statement, including recommended remediation, for a case-study control failure.

Module 17: Assembling the Authorization Package

- Lessons:
  - Required components of an authorization package
  - Coordinating inputs from scoping, implementation and assessment
  - Common authorization package deficiencies
- Applied activity: Learners build a checklist confirming a case-study authorization package is complete before submission.

Module 18: Risk Determination and the Authorizing Official's Decision

- Lessons:
  - Weighing residual risk against organizational tolerance
  - The authorizing official's decision options
  - Documenting and communicating the authorization decision
- Applied activity: Given a completed case-study authorization package, learners recommend a decision and justify it in writing.

Module 19: Plans of Action and Milestones

- Lessons:
  - Purpose and structure of a plan of action and milestones
  - Prioritizing and scheduling remediation
  - Tracking a plan of action and milestones to closure
- Applied activity: Learners draft one plan of action and milestones entry for an open finding, including a realistic milestone schedule.

Module 20: Designing a Continuous Monitoring Strategy

- Lessons:
  - Purpose of continuous monitoring in the risk management life cycle
  - Selecting metrics and monitoring frequency
  - Aligning the strategy with organizational risk tolerance
- Applied activity: Learners draft a monitoring frequency table for five control families based on a case-study system's risk level.

Module 21: Ongoing Assessment and Control Effectiveness Over Time

- Lessons:
  - Reassessing controls on an ongoing basis
  - Detecting control drift and degradation
  - Updating the system security plan based on monitoring results
- Applied activity: Given two monitoring snapshots of the same control taken months apart, learners identify signs of drift and recommend an update.

Module 22: Reporting Risk and Security Status to Leadership

- Lessons:
  - Building a risk and security status report
  - Tailoring reporting for technical and executive audiences
  - Feeding status reports back into governance decisions
- Applied activity: Learners rewrite one technical monitoring finding as a two-sentence executive summary suitable for a governance board.

Module 23: System Disposal, Reauthorization and Program Maturity

- Lessons:
  - Reauthorization triggers and timing
  - Secure system disposal and decommissioning

    - Maturing a risk management program over time
- Applied activity: Learners identify which of five described events would trigger reauthorization and which apply to disposal instead.