

CGE-Foundations

Exam Blueprint

Certified GRC Engineer, Foundations

GRC Engineering Club Training Academy

Instructor: AJ Yawn

Version 1.0 | November 2026

www.grcengclub.com

ABOUT THIS DOCUMENT

Purpose: This is the official guide to the Certified GRC Engineer, Foundations (CGE-Foundations) exam: what it covers, how it is weighted, and what you need to be able to do.

What it validates: A CGE-Foundations holder speaks the language of GRC. They can define, classify, and tell apart the terms used in governance, risk, controls, compliance, audit, and GRC engineering, and recognize the right term in a short workplace situation. They are not asked to design a program or write code.

Prerequisites: None. No coding background, cloud experience, GRC work history, or other CGE credential is required.

Cost: Free for active GRC Engineering Club members.

EXAM STRUCTURE AND FORMAT

Attribute	Details
Format	Computer-based, taken in the Academy. Open book.
Time limit	45 minutes
Total questions	30
Multiple choice	24 questions (4 options, one correct answer)
Scenario-based	6 questions (a short workplace situation, then one question; 4 options, one correct answer)
Passing score	70% (21 of 30)
Scoring	All questions count equally. No negative marking. Unanswered questions count as wrong.
Portfolio or capstone	None
Retake policy	14-day wait between attempts; maximum 3 attempts in any 12 months
Validity	365 days per certificate; 3-year credential (original plus two renewals, then a retake)

DOMAIN OVERVIEW

#	Domain	Weight	Questions	Focus
1	GRC Concepts	10%	3	What G, R, and C mean, the CIA triad, GRC, security, and audit, roles, the three lines model
2	Governance	15%	4	Policies, standards, procedures, guidelines, ownership, RACI, exceptions, oversight
3	Risk	20%	6	Asset, threat, vulnerability, risk, scoring, treatment, the risk register, vendor management
4	Controls	20%	6	Controls and objectives, control types, compensating and inherited controls, design and operating effectiveness
5	Compliance & Frameworks	15%	5	Law to standard, recognizing nine frameworks, scope, attestation, certification, mapping
6	Audit & Assurance	10%	3	Internal and external audit, independence, evidence, sampling, findings, Type 1 and Type 2
7	GRC Engineering Concepts	10%	3	Shared responsibility, APIs, version control, IaC, policy-as-code, continuous monitoring, at the definition level
Total		**100%**	**30**	

Risk and controls carry the most weight because every later concept is built on them. Question counts are the published weights applied to 30 questions.

DOMAIN 1: GRC CONCEPTS

Weight: 10% (3 questions) **Lessons:** 01_01, 01_02

Objectives

- 1.1 Define governance, risk, and compliance, and name the three parts of the CIA triad
- 1.2 Explain why GRC exists and how the three letters work together
- 1.3 Tell GRC, security, and audit apart
- 1.4 Place each role in the three lines model, and explain separation of duties

Terms in scope

Governance, risk, compliance, confidentiality, integrity, availability, three lines model, separation of duties, GRC analyst, compliance manager, risk manager, GRC engineer, CISO.

DOMAIN 2: GOVERNANCE

Weight: 15% (4 questions) **Lessons:** 02_01, 02_02

Objectives

- 2.1 Classify a statement as a policy, standard, procedure, or guideline
- 2.2 Explain how the four document types relate, and who approves a policy
- 2.3 Read a RACI chart and spot a row with a problem
- 2.4 Explain what an exception is, what it contains, and who approves it
- 2.5 Describe the role of a steering committee and the board

Terms in scope

Policy, standard, procedure, guideline, owner, Responsible, Accountable, Consulted, Informed, exception, steering committee, board of directors.

DOMAIN 3: RISK

Weight: 20% (6 questions) **Lessons:** 03_01, 03_02, 03_03, 03_04, 03_05

Objectives

- 3.1 Tell an asset, threat, vulnerability, risk, and incident apart in a short example
- 3.2 Score a risk on likelihood and impact, and tell qualitative from quantitative analysis
- 3.3 Tell inherent from residual risk, and appetite from tolerance
- 3.4 Choose a treatment option for a scenario: mitigate, transfer, avoid, or accept
- 3.5 Read a risk register row and explain each field
- 3.6 Walk through the vendor lifecycle and explain why vendors are tiered by criticality

Terms in scope

Asset, threat, vulnerability, risk, incident, likelihood, impact, heat map, qualitative, quantitative, FAIR, inherent risk, residual risk, appetite, tolerance, treatment, risk register, vendor inventory, tiering, due diligence, security questionnaire, data processing agreement, subprocessor, fourth party, ongoing monitoring, offboarding, TPRM.

DOMAIN 4: CONTROLS

Weight: 20% (6 questions) **Lessons:** 04_01, 04_02, 04_03, 04_04

Objectives

- 4.1 Define a control and tell a control objective from the control that meets it
- 4.2 Recognize a control description that can be tested
- 4.3 Classify any control by function and by nature
- 4.4 Recognize manual, automated, compensating, and inherited controls
- 4.5 Tell a design failure from an operating failure in a short scenario

Terms in scope

Control, control objective, control owner, control library, preventive, detective, corrective, deterrent, administrative, technical, physical, manual, automated, compensating, inherited, common, design effectiveness, operating effectiveness, walkthrough, continuous control monitoring.

DOMAIN 5: COMPLIANCE AND FRAMEWORKS

Weight: 15% (5 questions) **Lessons:** 05_01, 05_02, 05_03, 05_04

Objectives

- 5.1 Tell a law or regulation from a framework or standard, and explain why a company follows each
- 5.2 Match each commercial framework to who needs it and why
- 5.3 Match each federal framework to who needs it and why
- 5.4 Explain scope, tell attestation from certification, and describe why controls get mapped

Terms in scope

Law, regulation, framework, standard, SOC 2, Trust Services Criteria, ISO 27001, ISMS, PCI DSS, HIPAA, PHI, covered entity, business associate, GDPR, NIST CSF, NIST 800-53, FedRAMP, ATO, CMMC, scope, attestation, certification, control mapping, crosswalk.

DOMAIN 6: AUDIT AND ASSURANCE

Weight: 10% (3 questions) **Lessons:** 06_01, 06_02, 06_03

Objectives

- 6.1 Tell internal from external audit, and Type 1 from Type 2
- 6.2 Explain independence, and tell an assessment from an audit
- 6.3 Explain how an auditor goes from a population to a sample to a conclusion
- 6.4 Read an audit finding and explain the path to remediation

Terms in scope

Assurance, audit, independence, assessment, gap assessment, Type 1, Type 2, evidence, sufficient, appropriate, population, sample, completeness and accuracy, IPE, exception, deficiency, finding, unqualified and qualified opinion, management response, root cause, remediation, POA&M.

DOMAIN 7: GRC ENGINEERING CONCEPTS

Weight: 10% (3 questions) **Lessons:** 07_01, 07_02, 07_03

Objectives

- 7.1 Explain what a GRC engineer does and how it differs from traditional GRC
- 7.2 Define shared responsibility, API, IAM, least privilege, and version control
- 7.3 Define infrastructure as code, policy-as-code, continuous monitoring, and drift

Terms in scope

GRC engineering, compliance by design, cloud, shared responsibility model, API, IAM, least privilege, version control, Git, pull request, infrastructure as code, policy-as-code, continuous monitoring, drift.

BLOOM'S TAXONOMY DISTRIBUTION

Targets across the exam. The mix on any one attempt can vary slightly because questions are drawn from a larger bank.

Domain	Remember	Understand	Apply	Total
1. GRC Concepts	2	1	0	3
2. Governance	2	1	1	4
3. Risk	2	2	2	6
4. Controls	2	2	2	6
5. Compliance & Frameworks	2	2	1	5
6. Audit & Assurance	1	2	0	3
7. GRC Engineering Concepts	1	2	0	3
Total	**12 (40%)**	**12 (40%)**	**6 (20%)**	**30**

Level	What a question asks you to do
Remember	Recall a definition or name the term
Understand	Explain a term, tell two terms apart, or recognize an example
Apply	Use a term in a workplace situation, such as classifying a control or choosing a treatment

CERTIFICATION MAINTENANCE

- Each certificate is valid for 365 days. The credential runs three years: the original plus two renewals, then a retake.
- The renewal window opens 60 days before expiry and closes 30 days after.
- Qualify with 290 or more days of Club membership in the last 3 years, or 30 approved CPE hours in the last 12 months.
- The first renewal has no CPE requirement.

HOW TO PREPARE

- Watch the 24 lessons in order. About an hour of video.
- Work through the CGE-Foundations Study Guide one domain at a time, and answer the self-checks out loud.
- Read the CGE-Foundations Glossary from A to Z at least once.
- Take the free practice exam at cert.grcengclub.com/practice/cge-foundations: 20 questions with an explanation for every answer.
- Spend the most time on Domains 3 and 4. Together they are 40% of the exam.

Where it fits: CGE-Foundations is a standalone on-ramp and is not required for anything else. It is the recommended first step before CGE-P (Practitioner) or CGE-AUD (Auditor Specialty) for anyone new to the field.

Website: www.grcengclub.com **Email:** academy@grcengclub.com **Slack:** #studygroup_cge_certs