

CGE-Foundations

Study Guide

Certified GRC Engineer, Foundations

GRC Engineering Club Training Academy

Instructor: AJ Yawn

Version 1.0 | November 2026

www.grcengclub.com

HOW TO USE THIS STUDY GUIDE

About the certification

The Certified GRC Engineer, Foundations (CGE-Foundations) is the entry-level credential in the CGE family. It teaches the language of GRC from zero: what a control is, what a risk is, how a policy differs from a standard, and what an auditor means by a finding. There is no prerequisite, no coding, no labs, and no portfolio. It is free for active GRC Engineering Club members.

Who it is for

Career changers, students, and veterans moving into GRC. Analysts in their first year. Engineers who were just pulled into a SOC 2 or ISO 27001 project. Anyone in product, sales, legal, finance, or HR who sits in compliance meetings and wants to follow them.

How to study

- **Watch the lesson, then read its section here.** The course is 24 short videos, about an hour in total.
- **Learn the pairs.** Most missed questions come from two terms that sound alike. Each domain below ends with its traps.
- **Do the self-checks out loud.** If you can answer in one sentence without looking, you know the term.
- **Keep the glossary open.** The printable glossary has every term in the course in one line each.
- **Take the practice exam.** 20 questions with explanations at cert.grcengclub.com/practice/cge-foundations.

Suggested plan

Session	Do this	Time
1	Domains 1 and 2: videos, notes, self-checks	About 35 min
2	Domain 3: videos, notes, self-check	About 40 min
3	Domain 4: videos, notes, self-check	About 35 min
4	Domains 5 and 6: videos, notes, self-checks	About 45 min
5	Domain 7, glossary read-through, practice exam	About 45 min

The running example: Harbor

Harbor is a made-up payroll software startup. A big customer just asked it for a SOC 2 report and nobody there knows where to start. Every domain returns to Harbor, and the examples in this guide use it too.

EXAM OVERVIEW

Attribute	Details
Questions	30: 24 multiple choice and 6 scenario-based
Time	45 minutes
Pass score	70% (21 of 30)
Open book	Yes. You may use course materials.
Portfolio or capstone	None
Prerequisite	None. Complete every lesson to unlock the exam.
Retakes	14-day wait between attempts, up to 3 attempts in any 12 months
Validity	365 days per certificate. 3-year credential: the original plus two renewals, then a retake.
Cost	Free for active Club members

#	Domain	Weight	Questions	What to know cold
1	GRC Concepts	10%	3	G, R, and C; the CIA triad; GRC, security, and audit; the three lines
2	Governance	15%	4	The four document types; RACI; exceptions; oversight
3	Risk	20%	6	The four risk words; scoring; inherent and residual; treatment; the register; vendors
4	Controls	20%	6	Objective and control; function and nature; manual to inherited; design and operating
5	Compliance & Frameworks	15%	5	Law to standard; who needs which framework; scope; attestation and certification
6	Audit & Assurance	10%	3	Internal and external; Type 1 and Type 2; population to conclusion; findings
7	GRC Engineering Concepts	10%	3	What a GRC engineer does; shared responsibility; API; IaC; policy-as-code

Roughly 40% of questions ask you to remember, 40% to understand, and 20% to apply.

DOMAIN 1: GRC CONCEPTS (10%, 3 QUESTIONS)

1.1 What is GRC? (01_01)

GRC is how an organization decides what it's trying to protect, figures out what could go wrong, and proves it's doing what it said it would do. It exists because companies hold things that matter to other people. Harbor holds salaries, bank accounts, and Social Security numbers, and its customers can't walk in and inspect the place.

Letter	What it means	At Harbor, when a customer asks for SOC 2
Governance decides	Who's in charge, what the rules are, who answers when something breaks	Leadership decides who runs it and how much to spend
Risk prioritizes	What could go wrong, how likely, how much it would hurt	The team works out where Harbor is actually exposed
Compliance proves	Showing you follow the rules that apply: a law, a contract, or your own policy	The customer needs a SOC 2 report

CIA triad	Means	Broken when
Confidentiality	Only the right people can see the data	Someone leaks salaries
Integrity	The data is accurate and nobody tampered with it	A bug changes a paycheck amount
Availability	It's there when you need it	Payroll goes down on payday

1.2 Who does what (01_02)

Group	One-word job	Verbs to look for in a job posting
Security	Does: builds and runs the protections	Build, run
GRC	Directs and tracks the program	Track, assess, coordinate
Audit	Verifies independently and reports	Test, report

Three lines model	Job	Example
First line	Owns the risk	Engineers and the people running the business
Second line	Oversight and expertise	Risk and compliance teams
Third line	Independent assurance, reporting to the board	Internal audit

An outside auditor sits outside the company completely. Titles to know: GRC analyst, compliance manager, risk manager, GRC engineer, and CISO.

Traps

- Compliance without governance is nobody owning anything. Compliance without risk is a checklist that doesn't protect the business.
- Small companies blend roles. What you can't blend is the check itself: one person running a control and checking it breaks **separation of duties**.

Self-check

Cover the answers. Say yours out loud first, then compare.

1. Which letter of GRC answers the question "who is accountable if this breaks?"
Governance.

2. A backup job silently corrupts half of the employee records. Which part of the CIA triad failed?
Integrity. The records are no longer accurate.

3. Why can't Harbor's internal audit function report to the head of engineering?
It checks engineering's work, so it has to stay separate. Internal audit reports to the board.

DOMAIN 2: GOVERNANCE (15%, 4 QUESTIONS)

2.1 Policies, standards, procedures, and guidelines (02_01)

Document	Quick test	Mandatory?	Sounds like
Policy	Why, and what is required	Yes	All access to company systems must be protected with strong authentication.
Standard	What exactly	Yes	Passwords must be at least 14 characters.
Procedure	How	Yes, for whoever does the task	Step one, open the admin console. Step two, select the user.
Guideline	Should consider	No	Consider using a password manager.

Policies sit on top, approved by leadership and changed rarely. Everything underneath supports them. Auditors test you against what you wrote, so keep policies short and stable and put the numbers in standards.

2.2 Ownership, exceptions, and oversight (02_02)

RACI	Means	In Harbor's quarterly access review
Responsible	Does the work	IT lead
Accountable	Answers for the result. Only one per task.	Head of engineering
Consulted	Gives input before it's done	Compliance manager
Informed	Hears about it after	CEO

An **exception** is a documented, approved, time-limited decision to not meet a requirement. A good one names the reason, the risk, who approved it, what's being done in the meantime, and when it expires. Above all of this sits oversight: a steering committee reviews top risks and makes decisions, and the board is ultimately responsible.

Traps

- The word "must" with a number next to it usually means a standard.
- Two A's in a RACI row: nobody is truly accountable. No A at all: that task is going to get dropped.
- An owner doesn't do all the work. An owner answers for it.
- A permanent exception is just a broken rule with paperwork.

Self-check

Cover the answers. Say yours out loud first, then compare.

1. "Laptops must lock after 5 minutes of inactivity." Which document type, and how do you know?
A standard. It's specific, mandatory, and checkable with a yes or no.

2. What has to change first if leadership decides remote work is no longer allowed: the policy or the procedure?
The policy. It states the intent, and everything below may need to move to match.

3. An exception form has a reason, a risk, and an approver. What two things are still missing?
What's being done in the meantime, and the expiry date.

DOMAIN 3: RISK (20%, 6 QUESTIONS)

3.1 Asset, threat, vulnerability, risk (03_01)

Word	Means	At Harbor	Stolen laptop example
Asset	Anything of value you need to protect	The payroll database	The customer files on it
Threat	Something that could cause harm	A criminal group that steals financial data	A thief in the airport
Vulnerability	A weakness a threat could exploit	An unpatched server	No disk encryption
Risk	The chance a threat exploits a vulnerability and harms an asset, and how bad that would be	Attackers steal bank details, Harbor faces lawsuits and loses customers	A stolen laptop exposing customer files

Write any risk like this: **because of this weakness, this threat could do this, causing this harm.** An **incident** is a risk that actually happened.

3.2 Measuring risk (03_02)

Every risk is sized on **likelihood** (how probable) and **impact** (how bad). On a five-point scale, multiply them: Harbor's unpatched server is 3 x 5 = 15, high. A lost encrypted laptop is 4 x 2 = 8, medium. The server ranks first even though laptops go missing more often.

	Qualitative	Quantitative
Uses	Labels or simple scales, often on a heat map	Numbers, usually dollars
Strength	Fast, and gets a room talking	Executives can compare it with other business decisions
Weakness	The labels are opinions	Takes more data and effort
Example	High, or 15 out of 25	20 percent chance a year of a two million dollar loss. FAIR is the best-known method.

3.3 Treating risk (03_03)

Pair	First	Second
Inherent and residual	**Inherent:** the level of risk before any controls	**Residual:** what's left after your controls
Appetite and tolerance	**Appetite:** the amount and type of risk the organization is willing to take to reach its goals	**Tolerance:** how far things may vary around that line in practice

Treatment	Means	Harbor example
Mitigate	Reduce it by adding or fixing controls	Patch the server
Transfer	Shift the financial hit to someone else	Buy cyber insurance
Avoid	Stop doing the risky thing	Delete old employee records it no longer needs
Accept	Decide consciously to live with it, signed and written down	A low-risk wiki issue that costs more to fix than it could lose

3.4 The risk register (03_04)

The running list of an organization's risks and what's being done about each one. Usually a spreadsheet, and that's fine.

Field	Harbor's row
Risk ID and description	R-012: attackers exploit an unpatched server and steal employee bank details
Owner	Dana, head of engineering. A named person.
Likelihood, impact, inherent score	3, 5, 15 (high)
Controls and residual score	Weekly patching and a web application firewall; 8 (medium)
Treatment and action	Mitigate: move the server behind the VPN by March 31
Status and last reviewed	In progress; January

3.5 Vendor management (03_05)

You can outsource the work. You can't outsource the responsibility.

Lifecycle step	What happens
1. Inventory	List every vendor, what they do, and what data they touch
2. Tier	Critical if it holds sensitive data or would stop the business if it went down
3. Due diligence	Security questionnaire, plus a SOC 2 report or ISO 27001 certificate
4. Contract	Data processing agreement, breach notification timelines, the right to ask for evidence
5. Monitor	Yearly reviews, new reports, breach alerts for critical vendors
6. Offboard	Remove access; data returned or deleted

A **subprocessor** is a company your vendor uses to process your data. To you, that's a **fourth party**. TPRM and vendor risk management mean roughly the same thing in most companies.

Traps

- An unpatched server is a vulnerability. It becomes a risk statement once you add the threat and the harm.
- Transfer doesn't remove the risk or your accountability. Insurance moves the money and not the damage.
- Doing nothing without a decision is not acceptance.
- Accepted risk needs an owner with real authority. The bigger the risk, the higher the signature.
- The goal is never zero risk. It's the right amount of risk, on purpose.
- A vendor's report only helps if it covers the product you're buying, is recent, and you read the exceptions.

Self-check

Cover the answers. Say yours out loud first, then compare.

1. A former employee's account is still active. Name the vulnerability and the threat.
The active account is the vulnerability. The former employee, or anyone who gets that password, is the threat.

2. Risk A scores likelihood 2, impact 5. Risk B scores likelihood 4, impact 3. Which goes higher on the list?
Risk B: 12 against 10.

3. Residual risk is below appetite. Does anything have to happen next?
No treatment is required. Keep it in the register and review it on schedule.

4. A company closes a product line because the data it needs is too dangerous to hold. Which treatment?
Avoid.

5. Which register column tells you whether anyone is using the register?
Last reviewed.

6. Your vendor hosts your data with another company. What do you call that company?
A subprocessor of your vendor, and a fourth party to you.

DOMAIN 4: CONTROLS (20%, 6 QUESTIONS)

4.1 What is a control? (04_01)

A control is a safeguard an organization puts in place to reduce risk. It actually happens: a setting, a review, a lock on a door. If you can't name the risk it addresses, ask why you have it.

Term	Means	Harbor example
Control objective	The outcome you want	Only authorized people can access payroll data
Control	The thing you do to get there	MFA on every login; manager-approved access; a quarterly access review
Policy	A statement of what is required	Access must be protected

A good control description says **who does what, how often, using what, and what proof it leaves**. "Access is reviewed regularly" can't be tested. "Each quarter, the IT lead reviews all user access to the payroll system, removes anything no longer needed, and the head of engineering signs off in a ticket" can.

4.2 Control types (04_02)

Two labels sort almost any control. **Function** is what it does. **Nature** is what it's made of.

	Administrative (people, process)	Technical (systems)	Physical (places, hardware)
Preventive: stops it before	Security awareness training	MFA	A locked door
Detective: finds it during or after	A quarterly access review	Audit logs and alerts	A security camera
Corrective: fixes it and gets you back to normal	An incident response plan	A backup restore	Replacing a broken lock

You'll also see **deterrent**: it discourages bad behavior, like a warning sign. Strong programs mix functions. With only prevention, you won't know when it fails.

4.3 Manual, automated, compensating, inherited (04_03)

Label	Means	Harbor example
Manual	Needs a person. Flexible but slow, and people miss things.	Someone reviews an access list and signs off
Automated	Runs by itself. Consistent, with a clean record.	The system blocks any login without MFA
Compensating	A substitute when you can't meet a requirement the normal way. Same risk, at least as well.	The old payroll tool sits behind the VPN, which requires MFA, with weekly log review
Inherited	You get it from someone else. Also called common when shared across many systems.	AWS secures the data centers; Harbor points to AWS's audit reports

4.4 Design vs. operating effectiveness (04_04)

	Design effectiveness	Operating effectiveness
Question	If it runs exactly as written, would it address the risk?	Did it run that way, consistently, over time?
Failure looks like	The only reviewer is the person who granted the access	Q3 was skipped because the manager was on leave
Fix	Rewrite the control	Fix the execution: backups, reminders, automation
How it's tested	A walkthrough: talk to the owner, read it, follow one example	Proof from the whole period

Traps

- A policy is not a control. Auditors don't stop at the document.
- The same tool can do different jobs. Ask what the control's main job is.
- A quarterly access review is detective: it finds bad access that already exists.
- Yearly training doesn't compensate for missing MFA. It doesn't stop a stolen password from working.
- Test design first. If the design is broken, there's no reason to test whether it ran.

Self-check

Cover the answers. Say yours out loud first, then compare.

1. Turn this into a testable control: "Backups are checked often."
One answer: each month, the IT lead restores one backup of the payroll database to a test system and records the result in a ticket.

2. Label a badge reader on a server room door with both labels.
Preventive and physical.

3. Label a monthly report that a manager reads to spot unusual payments.
Detective and administrative.

4. A control covers every login except the admin back door. Design or operating failure?
Design. It can't do its job even when it runs perfectly.

5. Why does Harbor point to AWS's audit reports instead of testing the data centers?
Those controls are inherited. AWS runs them and its reports are the proof.

6. Which is easier to prove over a full year, a manual or an automated control, and why?
Automated. It runs the same way every time and leaves a clean record.

DOMAIN 5: COMPLIANCE AND FRAMEWORKS (15%, 5 QUESTIONS)

5.1 Law, regulation, framework, standard (05_01)

Type	Where it comes from	Example
Law	Passed by a government	HIPAA
Regulation	The detailed rule issued under a law, or directly by a regulator	GDPR
Framework	A structured set of practices for managing security or risk	NIST CSF
Standard	A formal, published set of requirements you can be measured against	ISO 27001

Obligations come from three places: **the government, your contracts, and your own commitments**. "Shall" and "must" mean required. "Should" usually means recommended.

5.2 and 5.3 The frameworks (05_02, 05_03)

Name	What it is	Who needs it
SOC 2	A CPA firm's report against the AICPA Trust Services Criteria: security, availability, processing integrity, confidentiality, privacy	Service companies, mostly SaaS, whose customers want proof
ISO 27001	International standard for an ISMS. An accredited body certifies you.	Companies with customers outside the US, among others
PCI DSS	Payment card data security standard, enforced through contracts	Anyone who stores, processes, or transmits card data
HIPAA	US law protecting health information (PHI)	Covered entities (hospitals, insurers) and their business associates
GDPR	EU privacy regulation about people's rights over their data	Anyone handling personal data of people in the EU, anywhere in the world
NIST CSF	Voluntary map with six functions: Govern, Identify, Protect, Detect, Respond, Recover	Any organization that wants a high-level view
NIST 800-53	Large catalog of security and privacy controls	US federal systems
FedRAMP	Authorizes cloud services; builds on 800-53	Cloud companies selling to US federal agencies
CMMC	US Department of Defense certification program	Defense contractors and their suppliers

ATO (authority to operate) is a federal official's formal decision to accept a system's risk and let it run. To spot what applies, look at **the customer, the data, and the country**.

5.4 Scope, attestation, certification, mapping (05_04)

	Attestation	Certification
Who	An independent auditor gives an opinion on your claims	An accredited body says you meet a standard
You get	A report	A certificate
Example	SOC 2	ISO 27001

Scope is what's being assessed: systems, people, locations, time period. **Control mapping** links one control to requirements in several frameworks, and a **crosswalk** is the list that shows how they line up. Test once, satisfy many.

Traps

- Nobody is "SOC 2 certified." SOC 2 is an attestation.
- PCI DSS and SOC 2 aren't laws, but contracts and customers can make them unavoidable.
- CSF is the map. 800-53 is the detailed parts list.
- GDPR follows the people whose data you hold. A US company can be covered.
- A report about a different product tells you nothing about the one you're buying.

Self-check

Cover the answers. Say yours out loud first, then compare.

1. A dental billing software company in Ohio. Which law applies, and what role does the company play?

HIPAA. It's a business associate of the dental practices it serves.

2. Harbor wants to sell to a federal agency. What does it need?

FedRAMP authorization for its cloud service.

3. Which document would you show a leader who wants one page on where the security program stands?

A NIST CSF view, organized by its six functions.

4. Harbor leaves its marketing website out of its SOC 2. Is that allowed?

Yes. That's a scope decision, as long as the scope is clear and covers what customers care about.

5. What does it mean to map one MFA control to three frameworks?

You build and test it once, and it counts toward the access requirements in all three.

DOMAIN 6: AUDIT AND ASSURANCE (10%, 3 QUESTIONS)

6.1 Audit basics (06_01)

	Internal audit	External audit
Who	Inside the company, reporting to the board	An outside firm
For	The board and leadership	Customers, regulators, or investors
Both rely on	Independence: no stake in the result	Independence: no stake in the result

	SOC 2 Type 1	SOC 2 Type 2
Covers	A single point in time	A period, often 3 to 12 months
Asks	Are the controls designed properly?	Are they designed properly, and did they operate?
Use	A first step, sometimes to close a deal	What most customers want

An **assessment** is a broader, often less formal review. A **gap assessment** finds what's missing before the real audit. An audit reaches a formal conclusion.

6.2 Evidence, populations, and sampling (06_02)

Step	Harbor's background check control
Population	All 60 hires in the audit period, exported from the HR system
Completeness and accuracy	How do I know this list is complete? (IPE: information produced by the entity)
Sample	The auditor picks 10
Test	For each one, was the check done before the start date?
Conclude	Ten for ten, no exceptions. The control worked.

Good evidence is **sufficient** (enough of it) and **appropriate** (relevant and reliable). A system export generally beats a cropped screenshot, and both beat someone saying it's fine.

6.3 Findings and remediation (06_03)

Word	Means
Exception	One instance where a control didn't work as described
Deficiency	A problem with the control itself, in design or operation
Finding	An issue the auditor formally reports
Unqualified opinion	The good one: no significant problems
Qualified opinion	Something serious enough to call out
Management response	The company explains what happened and what it's doing about it
Root cause	Why it failed. Fix that, not only the single miss.
POA&M	Plan of action and milestones: each weakness, owner, fix, and due date

Traps

- An **unqualified** opinion is the good one. The name's backwards.
- If you can't prove it, it didn't happen.
- A sample means nothing if the population behind it is incomplete.
- An audit exception is a failed test item. A policy exception is an approved decision. Same word, different things.

Self-check

Cover the answers. Say yours out loud first, then compare.

1. The auditor helped write the control they're now testing. What's missing?
Independence.

2. Why does an auditor ask how you generated a list before looking at what's on it?
To check completeness and accuracy. Items left off can never be sampled.

3. One of ten samples failed. Is that automatically a deficiency?
No. It's an exception. A pattern of them points to a deficiency.

DOMAIN 7: GRC ENGINEERING CONCEPTS (10%, 3 QUESTIONS)

7.1 What makes GRC engineering (07_01)

GRC engineering means using software practices to build and run governance, risk, and compliance. Controls are still controls and risk is still risk. What changes is how the work gets done. **Compliance by design** means building the rule into the system so the secure way is the default way.

	The old way	The engineered way
Evidence	A screenshot every quarter	A script that collects it
Database encryption	Someone screenshots the settings	A script checks every database, every day, and raises a ticket
Human judgment	Needed	Still needed: what's worth checking, and what a failed check means

7.2 and 7.3 The vocabulary (07_02, 07_03)

Term	Means	Why GRC cares
Shared responsibility	The provider secures the cloud itself. You secure what you put in it.	An open storage bucket is on you
API	How software talks to software	Evidence without a screenshot
IAM and least privilege	Who can do what; only the access needed to do the job	The base of access control
Version control	Tracks every change: who, when, why. Git is the standard tool.	Practically an audit trail
Pull request	A proposed change someone else reviews	Built-in approval and separation of duties
Infrastructure as code	Servers and networks described in text files. Terraform is the best-known tool.	Review and check it before it goes live
Policy-as-code	A rule in a form a machine can run	Blocks a bad change before it ships
Continuous monitoring	Checking controls automatically and constantly. Also called CCM.	You hear about drift that day
Drift	A system quietly changed from how it's supposed to be	What monitoring is there to catch

Traps

- Infrastructure as code **describes** the system. Policy-as-code **checks** it.
- Policy-as-code that blocks a change is preventive, technical, and automated. Continuous monitoring finds what already changed, so it's detective.
- Automation doesn't remove the need for GRC judgment.

Self-check

Cover the answers. Say yours out loud first, then compare.

1. A cloud provider's data center loses power and its backup fails. Whose side of the line?
The provider's. It secures the buildings, the hardware, and the core services.

2. What does a pull request give an auditor that an email approval might not?
The exact change, who proposed it, who reviewed it, and when, all in one history.

3. Yesterday's check passed. Today someone changed a setting by hand. What's the word, and what catches it?
Drift. Continuous monitoring catches it.

EXAM DAY

Before you start

- Complete every lesson, including the three reading lessons. The exam unlocks when they're all checked off.
- Take the practice exam and review the domain where you scored lowest.
- Read this guide's traps once more. They take ten minutes.
- Set aside 45 minutes. The timer runs on our server and closing the tab doesn't pause it.

During the exam

- 45 minutes for 30 questions is 90 seconds each. Most definition questions take far less.
- On a scenario, find the fact the question turns on, name the term yourself, then look for it in the answers.
- Flag anything you're unsure of and come back. Unanswered questions count as wrong.
- The exam is open book, but don't plan to look up every answer.

After the exam

- **Pass:** confirm the name for your certificate and it's issued straight away.
- **Not yet:** you get your score by domain. Wait 14 days, study those domains, and try again. Up to 3 attempts in any 12 months.
- **Renewal:** the window opens 60 days before your certificate expires 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. Your first renewal has no CPE requirement.

Glossary and next steps

The CGE-Foundations Glossary lists 156 terms in one line each, with the lesson that covers them: grcengclub.com/academy/CGE-Foundations_Glossary.pdf. If you want to build this, CGE-P (Practitioner) is next. If you audit, look at CGE-AUD (Auditor Specialty).

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