

CGE-Foundations

GRC Glossary

Certified GRC Engineer, Foundations

GRC Engineering Club Training Academy

Instructor: AJ Yawn

Version 1.0 | November 2026

www.grcengclub.com

HOW TO USE THIS GLOSSARY

156 terms, A to Z, in one plain line each. The number after a definition is the lesson that covers it: 03_01 is Domain 3, lesson 1. Terms marked Beyond the videos aren't taught in a lesson and won't be on the exam, but you'll hear them at work.

A

Acceptance (Accept): A treatment option: consciously deciding to live with a risk, approved by someone with the authority and written down. [03_03]

Access review: A periodic check that each person's access to a system is still needed, with anything extra removed. [04_02]

Accountable: The A in RACI: the one person who answers for the result of a task. [02_02]

Administrative control: A control made of people and process, such as a policy, training, or an access approval. [04_02]

API (application programming interface): The way software talks to software: a program asks a system a question and gets a structured answer. [07_02]

Assessment: A review of where things stand that is broader and often less formal than an audit. It finds gaps; an audit reaches a formal conclusion. [06_01]

Asset: Anything of value you need to protect, such as a database, source code, a laptop, or your reputation. [03_01]

Assurance: Justified confidence, from an independent check, that things are what they are claimed to be. [06_01]

ATO (authority to operate): The formal decision by a federal official to accept a system's risk and let it run. [05_03]

Attestation: An independent auditor's opinion on an organization's claims, delivered as a report. SOC 2 works this way. [05_04]

Audit: A structured, independent check of whether things are what they are claimed to be. [06_01]

Audit evidence: The information an auditor uses to reach a conclusion, such as a system export, log, ticket, configuration, or signed review. [06_02]

Audit opinion: The auditor's overall conclusion in a report. [06_03]

Audit trail: A record of who did what and when, kept so it can be checked later. [07_02]

Automated control: A control that runs by itself every time, such as a system that blocks any login without MFA. [04_03]

Availability: The part of the CIA triad that means data and systems are there when you need them. [01_01]

Avoidance (Avoid): A treatment option: stopping the activity that creates the risk, such as deleting data you no longer need. [03_03]

B

Board of directors: The body ultimately responsible for how the company handles risk. [02_02]

Business associate: A company that works with protected health information on behalf of a HIPAA covered entity. [05_02]

Business continuity: The ability and plan to keep critical operations running during a disruption. [Beyond the videos]

C

Certification: Confirmation from an accredited body that you meet a standard, shown by a certificate. ISO 27001 works this way. [05_04]

CIA triad: Confidentiality, integrity, and availability: the three properties most protection work comes down to. [01_01]

CISO (chief information security officer): The executive usually accountable for the whole security and GRC program. [01_02]

Cloud: Computing rented from a provider such as AWS, Microsoft Azure, or Google Cloud instead of run on your own servers. [07_02]

CMMC (Cybersecurity Maturity Model Certification): The US Department of Defense program for its contractors and their suppliers. [05_03]

Common control: An inherited control: one team's control that is shared across many systems. [04_03]

Compensating control: A substitute used when you cannot meet a requirement the normal way. It must address the same risk at least as well. [04_03]

Completeness and accuracy: The test of whether a list or report has everything it should and whether what it says is correct. [06_02]

Compliance: Proving you follow the rules that apply to you, whether from a law, a contract, or your own policy. [01_01]

Compliance by design: Building the rule into the system so the secure way is the default way. [07_01]

Compliance manager: The person who owns a compliance program such as SOC 2. [01_02]

Confidentiality: The part of the CIA triad that means only the right people can see the data. [01_01]

Consulted: The C in RACI: someone whose input is needed before the task is done. [02_02]

Continuous control monitoring (CCM): Checking controls automatically and constantly instead of once a quarter or once a year. Also called continuous monitoring. [07_03]

Control: A safeguard an organization puts in place to reduce risk: something that actually happens, such as a setting, a review, or a lock. [04_01]

Control description: A statement of who does what, how often, using what, and what proof it leaves behind. [04_01]

Control library: One list of every control with its owner, frequency, and evidence. Also called a control matrix. [04_01]

Control mapping: Linking one control to the requirements it satisfies in several frameworks, so you test once and satisfy many. [05_04]

Control objective: The outcome you want. The control is the thing you do to get there. [04_01]

Control owner: The named person who answers for a control. [04_01]

Corrective control: A control that fixes things and gets you back to normal, such as a backup restore, a patch, or an incident response plan. [04_02]

Covered entity: An organization HIPAA applies to directly, such as a hospital or a health insurer. [05_02]

Crosswalk: A list showing how requirements line up across frameworks. [05_04]

D

Data processing agreement (DPA): Contract terms covering how a vendor handles personal data on your behalf. [03_05]

Deficiency: A problem with a control itself, in how it is designed or how it operates. [06_03]

Design effectiveness: Whether a control, if it runs exactly as written, would actually address the risk. [04_04]

Detective control: A control that finds something during or after it happens, such as a log, an alert, or a camera. [04_02]

Deterrent control: A control that discourages bad behavior, such as a warning sign. [04_02]

Disaster recovery: The plan and process for restoring systems and data after a major outage. [Beyond the videos]

Drift: When a system quietly changes from how it is supposed to be. [07_03]

Due diligence: Checking out a vendor before you sign, usually with a security questionnaire and its SOC 2 report or ISO 27001 certificate. [03_05]

E

Encryption: Scrambling data so only someone with the right key can read it. [Beyond the videos]

Exception (audit): One instance where a control did not work as described. [06_03]

Exception (policy): A documented, approved, time-limited decision to not meet a requirement. [02_02]

External audit: An audit by an outside firm, usually for customers, regulators, or investors. [06_01]

F

FAIR (Factor Analysis of Information Risk): The best-known method for quantitative risk analysis in cybersecurity. [03_02]

FedRAMP (Federal Risk and Authorization Management Program): The program that authorizes cloud services for US federal agencies. It builds on NIST 800-53. [05_03]

Finding: The general term for an issue the auditor formally reports. [06_03]

Fourth party: A company your vendor relies on, such as a subprocessor. [03_05]

Framework: A structured set of practices for managing security or risk, such as NIST CSF. [05_01]

G

Gap assessment: A comparison of where you are against a framework, done to find what is missing before the real audit. [06_01]

GDPR (General Data Protection Regulation): The European Union's privacy regulation. It covers the personal data of people in the EU and can reach companies anywhere. [05_02]

Git: The standard tool for version control. GitHub is a popular place to host it. [07_02]

Governance: How decisions get made: who is in charge, what the rules are, and who answers when something breaks. [01_01]

GRC: Governance, risk, and compliance: how an organization decides what to protect, figures out what could go wrong, and proves it does what it said it would do. [01_01]

GRC analyst: The person who runs the day to day of GRC: evidence, questionnaires, and risk updates. [01_02]

GRC engineer: A person who builds software that automates governance, risk, and compliance work. [01_02]

GRC engineering: Using software practices to build and run governance, risk, and compliance. [07_01]

Guideline: An optional recommendation. Nobody fails an audit over one. [02_01]

H

Heat map: A grid that plots likelihood against impact, running from green to red. [03_02]

HIPAA: A United States law protecting health information. It applies to covered entities and their business associates. [05_02]

I

IAM (identity and access management): How you control who can do what in a system. [07_02]

Impact: How bad it is if a risk happens. [03_02]

Incident: A risk that actually happened. [03_01]

Independence: The auditor having no stake in the result. You cannot audit your own work or a control you helped design. [06_01]

Informed: The I in RACI: someone who hears about the task after it is done. [02_02]

Infrastructure as code (IaC): Describing servers and networks in text files instead of clicking around in a console. Terraform is the best-known tool. [07_03]

Inherent risk: The level of risk before any controls. [03_03]

Inherited control: A control you get from someone else, such as a cloud provider's data center security. [04_03]

Integrity: The part of the CIA triad that means data is accurate and nobody tampered with it. [01_01]

Internal audit: Independent auditors inside the company who report to the board. The third line. [06_01]

IPE (information produced by the entity): A list or report the company generates and gives the auditor, who checks it for completeness and accuracy. [06_02]

ISMS (information security management system): A whole program for managing security, not a list of tools. ISO 27001 sets the requirements for one. [05_02]

ISO 27001: The international standard for an information security management system. An accredited body certifies you against it. [05_02]

K

Key risk indicator (KRI): A measurement that warns you when a risk is rising. [Beyond the videos]

L

Law: A rule passed by a government. [05_01]

Least privilege: Giving people only the access they need to do the job. [07_02]

Likelihood: How probable a risk is. [03_02]

M

Management response: The part of a report where the company explains what happened and what it is doing about it. [06_03]

Manual control: A control that needs a person to do it, such as a manager reviewing an access list. [04_03]

MFA (multi-factor authentication): Requiring two or more kinds of proof to log in, such as a password and a code from an app. [02_01]

Mitigation (Mitigate): A treatment option: reducing a risk by adding or fixing controls. [03_03]

N

NIST: A US government agency, the National Institute of Standards and Technology, that publishes security guidance. [05_03]

NIST 800-171: The NIST requirements for protecting controlled unclassified information outside federal systems. CMMC Level 2 is based on it. [Beyond the videos]

NIST 800-53: A large catalog of security and privacy controls used across US federal systems. [05_03]

NIST CSF (Cybersecurity Framework): A voluntary framework with six functions: Govern, Identify, Protect, Detect, Respond, and Recover. [05_03]

O

Offboarding (vendor): Ending a vendor relationship by removing access and getting data returned or deleted. [03_05]

Ongoing monitoring (vendor): Watching critical vendors after signature with yearly reviews, new reports, and breach alerts. [03_05]

Operating effectiveness: Whether a control actually ran the way it was designed, consistently, over time. [04_04]

P

PCI DSS (Payment Card Industry Data Security Standard): The standard for anyone who stores, processes, or transmits card data, enforced through contracts with card brands and banks. [05_02]

Personal data: Information relating to a person who is identified or can be identified. GDPR's term. [Beyond the videos]

PHI (protected health information): The health information HIPAA protects. [05_02]

Physical control: A control that protects places and hardware, such as a badge, lock, or camera. [04_02]

PII (personally identifiable information): Information that can identify a person, alone or combined with other information. [Beyond the videos]

POA&M (plan of action and milestones): A list of each weakness, its owner, the fix, and the due date. Federal programs use it to track remediation. [06_03]

Policy: A high-level statement, approved by leadership, of what the organization requires and why. [02_01]

Policy-as-code: Writing a rule in a form a machine can run, so it can check changes automatically. [07_03]

Population: The complete set of items a control applies to. [06_02]

Preventive control: A control that stops something before it happens, such as MFA or a locked door. [04_02]

Procedure: The step-by-step how, written for the person doing the work. [02_01]

Pull request: A proposed change that someone else reviews before it is accepted. [07_02]

Q

Qualified opinion: An opinion that calls out something serious the auditor found. [06_03]

Qualitative analysis: Sizing risk with labels or simple scales, such as low, medium, high, or one to five. [03_02]

Quantitative analysis: Sizing risk with numbers, usually dollars. [03_02]

R

RACI: A chart showing who is Responsible, Accountable, Consulted, and Informed for each task. [02_02]

Regulation: The detailed rule issued under a law, or directly by a regulator. [05_01]

Remediation: Fixing the problem, starting with the root cause. [06_03]

Residual risk: The risk that is left after your controls are in place. [03_03]

Responsible: The R in RACI: the person who does the work. [02_02]

Risk: The chance that a threat exploits a vulnerability and harms an asset, and how bad that would be. [03_01]

Risk appetite: The amount and type of risk an organization is willing to take to reach its goals. [03_03]

Risk manager: The person who runs the risk process. [01_02]

Risk register: The running list of an organization's risks and what is being done about each one. [03_04]

Risk tolerance: How far the organization will let things vary around its risk appetite in practice. [03_03]

Risk treatment: What you decide to do about a risk: mitigate, transfer, avoid, or accept. [03_03]

Root cause: The underlying reason a control failed. [06_03]

RPO (recovery point objective): The most data, measured in time, you can afford to lose in an outage. [Beyond the videos]

RTO (recovery time objective): The longest a system can be down before it must be restored. [Beyond the videos]

S

Sample: The smaller set of items an auditor picks from the population to test. [06_02]

Scope: What is being assessed: which systems, people, locations, and time period. [05_04]

Security questionnaire: A list of questions about a vendor's security practices. [03_05]

Separation of duties: Splitting a task so one person does not both run something and check it. [01_02]

Shared responsibility model: The split where the cloud provider secures the cloud itself and you secure what you put in it. [07_02]

SOC 2: A report by a CPA firm on a service company's controls, measured against the AICPA Trust Services Criteria. [05_02]

SSP (system security plan): A document describing a system, its boundary, and how it meets its security requirements. [Beyond the videos]

Standard (external): A formal, published set of requirements you can be measured against, such as ISO 27001. [05_01]

Standard (internal): A mandatory, specific, measurable rule that makes a policy checkable with a yes or no. [02_01]

Steering committee: A regular meeting where leaders review top risks and make decisions. [02_02]

Subprocessor: A company your vendor uses to process your data. [03_05]

T

Tabletop exercise: A discussion-based practice run of an incident or disaster. [Beyond the videos]

Technical control: A control that lives in systems, such as encryption, a firewall, or MFA. [04_02]

Third party: Anyone outside your company who you do business with. A vendor is the most common kind. [03_05]

Third-party risk management (TPRM): Managing the risk that comes from outside companies. In most companies it means roughly the same as vendor risk management. [03_05]

Threat: Something that could cause harm, such as a criminal group, a careless employee, or a flood. [03_01]

Three lines model: The Institute of Internal Auditors model: the first line owns risk, the second provides oversight and expertise, the third is internal audit. [01_02]

Tiering: Sorting vendors by how critical they are, so the riskiest get the most scrutiny. [03_05]

Transfer: A treatment option: shifting the financial hit to someone else, such as with cyber insurance. You keep the accountability. [03_03]

Trust Services Criteria: The criteria for SOC 2: security, availability, processing integrity, confidentiality, and privacy. [05_02]

Type 1 report: A SOC 2 report on whether controls are designed properly at a single point in time. [06_01]

Type 2 report: A SOC 2 report on whether controls are designed properly and actually operated over a period, often 3 to 12 months. [06_01]

U

Unqualified opinion: The good opinion: the auditor found no significant problems. [06_03]

V

Vendor inventory: A list of every vendor, what they do, and what data they touch. [03_05]

Vendor management: Controlling third-party risk across the vendor lifecycle: inventory, tier, due diligence, contract, monitor, offboard. [03_05]

Version control: Tracking every change to a file: who changed it, when, and why. [07_02]

Vulnerability: A weakness a threat could exploit. [03_01]

W

Walkthrough: Testing design by talking to the owner, reading the description, and following one example through. [04_04]