CAREER ROADMAP

How to Become a GRC Analyst: A Complete Roadmap

A complete, no-code roadmap to landing your first GRC Analyst role: the frameworks, the skills, the certifications, and the 5-step path from zero experience to job offer.

IN THIS ROADMAP

Governance, Risk & Compliance (GRC) is one of the fastest-growing fields in cybersecurity, and you don't need to write a single line of code to succeed in it. This roadmap walks you through everything you need to land your first GRC role, from zero experience to job offer.

WHAT IS A GRC ANALYST?

A **GRC analyst** translates regulations, frameworks, policies, cybersecurity requirements and business risks into repeatable processes and controls, then helps determine whether those controls are actually working, documents the evidence, identifies the gaps and tracks remediation to closure. It sits at the intersection of the business and cybersecurity. Rather than hacking or building systems, GRC professionals:

- Develop and manage **cybersecurity policies**
- Conduct **risk assessments** to identify vulnerabilities
- Ensure the organization stays **compliant** with government and industry regulations
- Collaborate across departments to align security practices with standards

THE GRC WORKFLOW

Requirement → Risk → Control → Evidence → Testing → Remediation → Reporting

Every GRC job is this loop, running continuously. Learn the loop and the job titles stop mattering.

THE GRC TOOLKIT

GRC platform + ticketing + evidence repository + spreadsheets + reporting + collaboration

Six categories. The vendor names change every few years; the categories do not.

THE GRC SKILL STACK

Risk + Controls + Cybersecurity + Compliance + Audit + Communication + Technology

Nobody arrives with all seven. Most people arrive with two and build the rest on the job.

This role is especially critical in industries that handle sensitive data — **finance, healthcare, and technology** — where the cost of non-compliance can mean massive fines and reputational damage.

Key frameworks you'll work with

Framework / Standard	What it covers
NIST	U.S. federal cybersecurity standards & risk management
ISO 27001	International information security management

Framework / Standard	What it covers
HIPAA	Healthcare data privacy and security (U.S.)
GDPR	Data privacy regulation (European Union)
PCI DSS	Payment card industry data security
SOC 2	Service organization controls for data trust

SKILLS YOU NEED

Soft skills (critical)

- **Communication** — you'll translate technical concepts for non-technical audiences and work across the whole organization
- **Critical thinking** — reviewing policies and identifying risks requires analytical reasoning, not just checklist compliance
- **Attention to detail** — audits, documentation, and compliance assessments leave no room for missed details

Technical knowledge (foundational)

You won't be coding, but you need to understand:

- General **networking concepts** and how systems communicate
- **Cloud security** fundamentals (AWS, Azure, GCP basics)
- How different teams and tools operate within an organization
- Common **GRC tools**: ServiceNow, OneTrust, Archer, Jira, Excel/Google Sheets

THE 5-STEP GRC ANALYST ROADMAP

Step 1 — Learn the fundamentals

Build a solid foundation in cybersecurity basics before diving deep into GRC-specific content.

- **Free resources:** cybersecurity/GRC YouTube channels, industry publications (ISACA, the NIST website), and free courses on Coursera, LinkedIn Learning, or Udemy.
- **Recommended starting certification:** the **Google Cybersecurity Professional Certificate** (Coursera) — beginner-friendly, no prior experience required.
- **GRC-specific learning:** start reading up on SOC 2, ISO 27001, and NIST, and learn what audits and compliance teams actually do day-to-day. The GRC Certifications Guide breaks down every credential and its salary impact.

Step 2 — Get practical experience

You don't need a job to build experience. Create your own.

- Work with **sample audit templates** — download real ones and practice filling them out
- Draft **cybersecurity policies** based on actual frameworks (NIST, ISO)
- Complete **risk-assessment and compliance checklists** on practice scenarios
- **Volunteer** to help a small business or nonprofit with basic compliance needs
- Join **online GRC projects** or community challenges

These projects become portfolio pieces you can reference on your resume and in interviews.

Step 3 — Get certified

Certifications validate your knowledge and signal seriousness. Work through them in order — full details and salary data are in the GRC Certifications Guide.

Level	Certification	Why it matters
Beginner	Google Cybersecurity Professional Cert	No-experience entry point, foundational knowledge
Foundational	CompTIA Security+	Required or preferred for nearly every entry-level cyber role
GRC-specific	CRISC	Risk-focused, highly respected in GRC
GRC-specific	CGRC	Directly aligned with GRC roles
Advanced	CISA	Industry gold standard for audit and assurance
Advanced	CISM	Management-level, great for senior GRC roles

Step 4 — Optimize your resume & LinkedIn

Resume: list all transferable skills (project management, policy writing, analysis, communication); include every self-study project; use keywords from job postings (risk assessment, compliance, audit, NIST, ISO, policy development); and highlight certifications prominently.

LinkedIn: write a headline with "GRC" and your target title (e.g. *Aspiring GRC Analyst | CompTIA Security+*), add certifications to your profile, post about what you're learning, and connect with GRC professionals and hiring managers.

Step 5 — Apply & network

Job titles to search: GRC Analyst, Compliance Analyst, Risk Analyst, IT Auditor, Information Security Analyst, Cybersecurity Risk Analyst.

Start applying now — you can **browse live GRC Analyst and compliance roles on GRC Careers**, our specialized, hand-reviewed board for governance, risk, compliance, and AI-governance jobs. New leadership roles are added weekly.

Where to network: LinkedIn (join GRC and cybersecurity groups), Discord & Reddit communities (r/cybersecurity, GRC servers), conferences and meetups (ISACA, local cybersecurity events), and the professional bodies **ISACA** and **(ISC)²**.

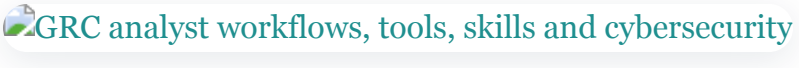
Pro tip: don't wait until you feel "ready" to apply. Start applying for entry-level roles while you're still studying — the interview process itself is a learning experience, and many employers hire for potential.

AT A GLANCE: YOUR GRC ROADMAP

Step	Action	Timeline (est.)
1	Learn cybersecurity & GRC fundamentals	1–2 months
2	Build practical experience through projects	Ongoing
3	Earn Google cert → Security+ → GRC certs	3–9 months
4	Optimize resume and LinkedIn	1–2 weeks
5	Apply for jobs and actively network	Ongoing

WHY GRC IS WORTH PURSUING

GRC sits at a rare crossroads: it requires **business acumen, analytical thinking, and cybersecurity knowledge** — but not deep technical expertise. That makes it one of the most accessible entry points into cybersecurity, and one of the most stable long-term career paths as regulations keep growing worldwide. Companies across every industry are under mounting pressure to comply with increasingly complex regulations, and skilled GRC professionals aren't just in demand — they're essential.



The four things every GRC analyst posting is really asking about: the GRC workflow you run, from requirement through risk, control, evidence, testing and remediation to reporting; the GRC tools and automation skills you run it with; the GRC and cybersecurity skills you bring; and the cybersecurity compliance domains you cover, from access control and IAM to cloud security, vulnerability management and incident response. Ready to apply it? See open GRC analyst jobs.

THE GRC ANALYST WORKFLOW

Job descriptions describe GRC in nouns. The work is a loop, and once you can see the loop you can read any posting and know what you would actually be doing on a Tuesday.

1. **Identify the requirement.** It arrives from a regulator, a customer contract, a framework the company adopted, a cybersecurity standard, or an internal policy. Somebody has to notice it and write it down.
2. **Map the requirement to a control.** Usually a control already exists that partly covers it. Mapping is the skill of recognizing that ISO 27001 A.9.2.3 and SOC 2 CC6.1 and your internal access policy are all asking one company to do one thing.
3. **Assign an owner.** A control without a named human is a control that does not operate. This step causes more friction than any other, because owners rarely volunteer.
4. **Collect evidence.** A screenshot, a config export, an access review, a signed approval. Evidence proves the control ran, not that it exists on paper.
5. **Test the evidence.** Sample it, check dates, check completeness, check whether it covers the whole population or just the easy part of it.
6. **Document the finding.** Gap, exception, or control failure, with a severity and a rationale someone can defend to an auditor.
7. **Assign remediation.** Owner and due date, tracked in the same system engineering already uses, not in a spreadsheet only you open.
8. **Track to closure.** Chase it. This is most of the job that nobody puts in the job description.
9. **Report.** Turn the whole thing into something a leadership team can make a decision from, in one page.

Then a requirement changes, a vendor changes, or a system changes, and it runs again. GRC is workflow-driven work, which is why GRC tools and automation skills have become the fastest-appreciating thing on a GRC resume.

WHAT DOES A GRC ANALYST DO EACH DAY?

A representative day, drawn from what the postings on our GRC analyst jobs hub actually ask for:

- **8:30** Review overdue remediation items and anything that changed on the risk register overnight.
- **9:30** Meet with IT or cybersecurity about evidence for an access control assessment. Half this meeting is explaining why last quarter's screenshot will not work again.
- **11:00** Review a new vendor's security questionnaire and decide what to escalate.
- **1:00** Map a set of ISO 27001 or NIST requirements against controls that already exist, and flag the genuine gaps.
- **2:30** Test documentation a control owner supplied, and send half of it back.
- **3:30** Update findings and remediation status in the GRC platform.
- **4:30** Draft the risk and compliance reporting that goes up to management.

Notice how little of it is reading regulations. Most GRC work is chasing, testing, documenting and translating.

GRC TOOLS ANALYSTS USE

Learn the categories rather than the logos. Products get acquired and renamed; what each category does for the workflow above has not changed in fifteen years.

Tool category	What the analyst uses it for
GRC platforms	Risks, controls, assessments, issues and reporting in one place
Audit and evidence platforms	Evidence requests, control testing, audit readiness
Third-party risk tools	Vendor assessments and security questionnaires
Ticketing and workflow systems	Findings and remediation tracking, in engineering's own queue
Document repositories	Policies, procedures, standards and stored evidence
Reporting and BI tools	Dashboards and management reporting
Spreadsheets	Control matrices, risk registers, and every analysis the platform cannot do yet

In practice you will see ServiceNow IRM, Archer, LogicGate, OneTrust, AuditBoard, Vanta and Drata named in postings, alongside Jira, Excel or Google Sheets, SharePoint and Power BI. Do not wait to be trained on one. Most of these have free tiers or trials, and being able to say you have configured a control library and run a test cycle in any of them puts you ahead of candidates who have only read about them.

GRC SKILLS EMPLOYERS LOOK FOR

Two stacks, and postings weight them about evenly. People underestimate the second one.

Technical and domain skills

- Risk assessment and risk register management
- Control design, control mapping and control testing
- Evidence collection and validation
- Compliance monitoring and audit readiness
- Policy and standards management
- Issue and remediation management
- Third-party and vendor risk management
- Regulatory interpretation
- Cybersecurity fundamentals and identity and access management concepts
- Data privacy fundamentals
- Cloud and SaaS risk
- Incident response governance
- Reporting and dashboards

Business skills

- Analytical thinking, and the judgment to know when an exception actually matters
- Technical writing and documentation, because in GRC the document is the control
- Stakeholder management with people who see you as overhead
- Interviewing control owners without putting them on the defensive

- Project management and prioritization
- Executive communication, and translating a technical issue into a business risk

If you are coming from another field, see which of these you already have in the cybersecurity and IT GRC career guides. Most career changers are further along than they think.

HOW DOES A GRC ANALYST WORK WITH CYBERSECURITY?

GRC is not separate from cybersecurity. In most organizations it is the governance and assurance layer wrapped around cybersecurity operations, and the two functions are usually in the same reporting line.

Take multifactor authentication. A security engineer configures it. The GRC analyst determines which framework or policy requires it, verifies it is implemented across the systems in scope rather than just the easy ones, reviews evidence that it operates, documents the exceptions where it does not, and tracks those exceptions to closure. Neither role can produce a defensible security program alone.

The same division of labour repeats across vulnerability management, privileged access, logging and monitoring, incident response, encryption, cloud security, change management, backup and recovery, and vendor security. If you already work in security operations, you have half of this job. See cybersecurity compliance and IT GRC jobs for what those postings currently pay and ask for.

FRAMEWORKS GRC ANALYSTS WORK WITH

You will not learn all of these. You will learn one properly and map the rest against it.

- **Cybersecurity:** NIST CSF, NIST SP 800-53, CIS Controls, ISO/IEC 27001, SOC 2, PCI DSS
- **Risk and governance:** COSO, ISO 31000
- **Privacy and regulated environments:** GDPR, HIPAA, and whatever your sector regulator requires
- **AI governance:** the NIST AI Risk Management Framework, ISO/IEC 42001, and the EU AI Act

That last group is the one worth getting ahead of. It is where new GRC headcount is being created, and almost nobody has five years of experience in it yet. See AI governance jobs and the career roadmaps for how the crossover works.

WHAT A GRC ANALYST ACTUALLY PRODUCES

If you want to picture the job, picture the artifacts. Over a year, a GRC analyst creates or maintains:

- Risk registers and risk assessments
- Control matrices and control libraries
- Compliance mappings across overlapping frameworks
- Policies and standards
- Audit evidence packages
- Findings registers and remediation plans
- Documented exceptions with compensating controls
- Vendor assessments and security questionnaire responses
- Compliance dashboards and executive risk reports

This list is also your portfolio plan. Build one of these properly for a framework you care about and you have something to walk an interviewer through, which beats a certificate on its own.

WHERE AUTOMATION AND AI ARE CHANGING THE WORKFLOW

Not hype, and not a threat to the job. Automation is eating the collection half of the loop and leaving the judgment half alone.

Tools now help with evidence collection, control mapping, regulatory change monitoring, questionnaire responses, document review, policy comparison, issue classification, reporting, and continuous control monitoring. What no tool

decides is whether a piece of evidence is actually valid, whether a control genuinely addresses the risk it is mapped to, whether an exception matters, and what the organization should do about it.

That is the whole argument for this career. The clerical part of GRC is being automated; the judgment part is being hired for. Analysts who can configure the automation and exercise the judgment are the ones getting promoted.

CAREER PATHS INTO AND OUT OF GRC

Almost nobody starts in GRC. The common feeder routes:

- Internal audit or external audit → GRC analyst
- Cybersecurity or IT operations → GRC analyst
- Compliance or legal and regulatory → GRC analyst
- Privacy → GRC analyst
- Risk management → GRC analyst
- Project or program management → GRC analyst

And out of it, either up the generalist ladder or into a specialism:

- **Generalist:** senior GRC analyst → GRC manager → director of GRC
- **Specialist:** cyber risk, third-party risk, security assurance, IT audit, privacy, compliance, AI governance, enterprise risk, or GRC program management

AI governance is the specialism with the steepest demand curve right now, and GRC analyst is the most common seat people move into it from. Ready to look? Browse open GRC analyst jobs, search everything at once with Super Search, or drill the frameworks with 592 free certification practice questions.

FREQUENTLY ASKED QUESTIONS

Do you need to code to be a GRC Analyst?

No. GRC is one of the few cybersecurity paths that does not require coding. You need to understand networking, cloud security basics, and how organizations work, but the job is about policy, risk assessment, compliance, and communication rather than writing code.

What certifications do GRC Analysts need?

Start with the Google Cybersecurity Professional Certificate and CompTIA Security+ for foundations, then move to GRC-specific certs like CRISC or CGRC, and advanced credentials like CISA or CISM for senior roles.

How long does it take to become a GRC Analyst?

Most people can become interview-ready in 3 to 9 months: 1-2 months on fundamentals, ongoing hands-on projects, and 3-9 months working through the certification ladder while applying for entry-level roles.

Where can I find GRC Analyst jobs?

Browse live GRC Analyst, compliance, and risk roles on GRC Careers (ai-governance-jobs.com), a specialized, hand-reviewed board for governance, risk, compliance, and AI-governance careers.

What is the GRC analyst workflow?

Requirement, risk, control, owner, evidence, test, finding, remediation, reporting, then it repeats. Every GRC job is that loop running continuously. Once you can see the loop, you can read any GRC posting and know what the day actually looks like.

What GRC tools should I learn first?

Learn the categories before the logos: GRC platform, audit and evidence platform, third-party risk tool, ticketing system, document repository, reporting tool, and spreadsheets. In postings you will see ServiceNow IRM, Archer, LogicGate, OneTrust, AuditBoard, Vanta and Drata alongside Jira, Excel and Power BI. Several have free tiers, so configure a control library and run a test cycle in one of them rather than waiting to be trained.

What GRC skills do employers actually screen for?

Two stacks weighted about evenly. Technical: risk assessment, control design, control mapping, control testing, evidence collection, compliance monitoring, audit readiness, policy management, remediation tracking, third-party risk, and cybersecurity and privacy fundamentals. Business: technical writing, documentation, stakeholder management, interviewing control owners, prioritization, and translating a technical issue into a business risk. Career changers usually underestimate how much of the second stack they already have.

Is GRC part of cybersecurity?

It is the governance and assurance layer around cybersecurity, usually in the same reporting line. A security engineer configures multifactor authentication; a GRC analyst determines which framework requires it, verifies it covers the systems in scope, reviews the evidence that it operates, documents the exceptions and tracks them to closure. Neither function produces a defensible program alone.

Will AI and automation replace GRC analysts?

Automation is taking the collection half of the workflow, not the judgment half. Tools now handle evidence collection, control mapping, regulatory change monitoring, questionnaire responses and continuous control monitoring. No tool decides whether evidence is valid, whether a control genuinely addresses its risk, whether an exception matters, or what the organization should do about it. Analysts who can configure the automation and exercise the judgment are the ones being promoted.

What jobs do people move into after GRC analyst?

Either up the generalist ladder, senior GRC analyst to GRC manager to director of GRC, or sideways into a specialism: cyber risk, third-party risk, security assurance, IT audit, privacy, compliance, enterprise risk, GRC program management, or AI governance. AI governance has the steepest demand curve right now and GRC analyst is the most common seat people move into it from.

This roadmap is a free resource from GRC Careers.
Read the latest version, and find live GRC Analyst jobs, at **ai-governance-jobs.com/ai-governance-career-guides/how-to-become-a-grc-analyst** · A resource from **GRC Careers**