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.

A free career roadmap from GRC Careers · AGJ, the AI governance job board
Read the latest version, and browse live GRC Analyst jobs, at **ai-governance-jobs.com/guides/how-to-become-a-grc-analyst**

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** sits at the intersection of 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

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
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.

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.