CAREER ROADMAP

# How to Get a Cybersecurity GRC Job: 2026 Career Guide

Learn how to enter cybersecurity governance, risk and compliance, including roles, frameworks, salaries, certifications and transition paths.

IN THIS ROADMAP

Cybersecurity GRC professionals connect security work with business objectives, risk decisions and external requirements. They develop policies, assess cyber risk, map controls, prepare for audits and help leaders understand whether security practices are appropriate and defensible.

## KEY TAKEAWAYS

- Cybersecurity GRC is a strong route into security for people with audit, compliance, policy, legal, operations or project-management experience.
- Coding is not required for every role, but professionals must understand security concepts and how controls operate.
- The BLS reported a $124,910 median for information security analysts in May 2024 and projects 29 percent growth from 2024 to 2034. That occupation is a useful benchmark, not a perfect proxy for every GRC job.

## WHAT IS GRC IN CYBERSECURITY?

Governance establishes security direction and accountability. Risk management identifies and prioritizes threats to business objectives. Compliance maps security practices to laws, standards, contracts and customer expectations.

Cybersecurity GRC professionals translate between technical teams, auditors, regulators, customers and executives. Their value comes from connecting controls with evidence and business decisions.

## COMMON CYBERSECURITY GRC JOB TITLES

1. GRC analyst
2. Security compliance analyst
3. Cyber risk analyst
4. IT risk analyst
5. Third-party cyber risk analyst
6. Security assurance manager
7. IT auditor
8. Cloud compliance specialist
9. GRC program manager
10. Director of GRC

## WHAT DOES A CYBERSECURITY GRC PROFESSIONAL DO?

- Maintain security policies, standards and control libraries.
- Conduct cybersecurity and third-party risk assessments.
- Map controls to frameworks and customer requirements.
- Collect and review audit evidence.
- Coordinate SOC 2, ISO 27001, PCI DSS, HIPAA or government assessments.
- Track findings, exceptions and remediation.
- Prepare risk and compliance reporting.
- Support security questionnaires and customer trust programs.
- Advise teams on control design and implementation.
- Govern emerging risks involving cloud services, vendors and AI.

## FRAMEWORKS AND TOOLS TO KNOW

Candidates do not need to memorize every framework. They should understand how requirements, controls, evidence and testing connect.

Common frameworks include NIST Cybersecurity Framework, NIST SP 800-53, ISO/IEC 27001, SOC 2 Trust Services Criteria, PCI DSS, CIS Controls, HIPAA Security Rule and FedRAMP requirements.

Common tools include ServiceNow IRM, Archer, LogicGate, OneTrust, AuditBoard, Vanta, Drata, spreadsheets, ticketing systems and evidence repositories.

## SKILLS EMPLOYERS LOOK FOR

- Security-control knowledge
- Risk assessment
- Framework mapping
- Audit evidence and testing
- Policy writing
- Vendor assessment
- Issue and remediation management
- Clear technical writing
- Stakeholder facilitation
- Basic cloud, identity, network and incident-response literacy

## SALARY AND OUTLOOK

The figures below are calculated from the 59 live Cybersecurity GRC postings on AI-Governance-Jobs.com, of which **52** publish a salary range. This is original market data from our own board, not a survey and not an editorial estimate.

| Level | Median midpoint | Middle half | Postings |
|---|---|---|---|
| Mid-level | **$132k** | $113k – $153k | 48 |

**Representative titles in this sample:** IT Cybersecurity Specialist, IT CYBERSECURITY SPECIALIST, SUPERVISORY IT CYBERSECURITY SPECIALIST, INFORMATION SECURITY SPECIALIST, Information Security Specialist, Supervisory IT Cybersecurity Specialist, Information Technology Specialist, Interdisciplinary.

### ▶ Methodology and cautions

## HOW TO GET A CYBERSECURITY GRC JOB

1. **Learn security fundamentals.** Understand access control, vulnerabilities, incidents, encryption, networks, cloud and system change.
2. **Learn one framework.** Map a small system to NIST CSF or ISO 27001 and identify evidence for selected controls.
3. **Practice risk assessment.** Write a clear risk statement with asset, threat, vulnerability, impact, likelihood, control and owner.
4. **Create work samples.** Build a control matrix, vendor questionnaire review, policy or audit-readiness plan.
5. **Translate your prior background.** Audit, compliance, legal, quality, project and IT operations experience can all be relevant.
6. **Target realistic entry roles.** Security compliance, third-party risk, audit support and GRC analyst roles are common bridges.

## CERTIFICATIONS

- ISC2 Certified in Cybersecurity or CompTIA Security+ for fundamentals.
- ISC2 CGRC for governance, risk and compliance.
- ISACA CISA for audit.
- ISACA CRISC for risk.
- ISACA CISM or ISC2 CISSP for experienced managers.
- Cloud-provider fundamentals and security credentials for cloud compliance.

Certifications are most effective when paired with work samples and an ability to discuss how a control works in practice.

## REMOTE WORK

Cybersecurity GRC is compatible with remote delivery because interviews, evidence collection, questionnaires and control tracking are frequently managed through shared systems. Remote availability should still be measured from current postings. It should not be described as the universal default without a defined dataset and date.

Remote candidates need especially strong documentation, follow-through and stakeholder-management habits because much of their work crosses teams and time zones.

## SOURCES AND UPDATE NOTES

- BLS Occupational Outlook Handbook: Information Security Analysts
- NIST Cybersecurity Framework
- NIST AI Risk Management Framework
- GRC Cybersecurity Careers article referencing AI-Governance-Jobs.com

**Internal links for publication:** Cybersecurity & IT GRC Jobs, Cybersecurity Risk Analyst guide, Third-Party Cyber Risk Manager guide, Security Compliance Manager guide, certification comparison and job alerts.

## FREQUENTLY ASKED QUESTIONS

### Is cybersecurity GRC technical?

It is technically informed. Many roles do not require software development, but professionals must understand systems, security controls and technical evidence.

### Can I enter cybersecurity through GRC?

Yes. GRC can be a strong entry route for people with audit, compliance, policy, legal, operations or project experience who add security fundamentals.

### Do GRC analysts need to code?

Usually not. Scripting and data skills can help with automation and analysis, but most roles emphasize controls, risk, evidence and communication.

### What certification should a beginner earn?

Security+ or ISC2 Certified in Cybersecurity can establish fundamentals. CGRC may suit candidates specifically targeting governance and compliance work.

### Is GRC less important than technical security?

No. Technical controls without ownership, risk decisions, policy and evidence are difficult to sustain or defend.

### What is a GRC platform?

It is software used to manage risks, controls, policies, assessments, evidence, issues and reporting.

### Can an IT auditor move into cybersecurity GRC?

Yes. IT audit is one of the strongest feeder backgrounds because it builds control, evidence and testing skills.

### How is AI changing cybersecurity GRC?

Teams must govern AI use, assess AI vendors, address AI-enabled threats and determine whether existing security controls remain adequate.

---

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