JOB DESCRIPTION TEMPLATE

Cybersecurity Compliance Analyst

Helps the organization meet its security control obligations by mapping requirements, collecting evidence, and supporting audits and certifications.

Department	Information Security / Security GRC / Compliance
Reports to	Security Compliance Manager / GRC Manager / CISO
Location	Remote / Hybrid / On-site
Employment type	Full-time
Experience	2 to 5 years

POSITION OVERVIEW

The Cybersecurity Compliance Analyst supports the organization's security compliance program, ensuring the organization meets the control requirements of applicable frameworks, regulations, and customer commitments. This role maps requirements to controls, collects evidence, tracks gaps, and helps the business stay audit-ready.

Working alongside security engineers, IT, and control owners, the analyst runs control assessments, coordinates audits and certifications, and keeps compliance documentation current. The role turns security frameworks into practical, repeatable evidence and reporting.

This is a hands-on role for a security-minded professional who enjoys structure, documentation, and working across teams to close gaps.

KEY RESPONSIBILITIES

FRAMEWORK AND CONTROL MAPPING

- Map security requirements to a unified control set.
- Maintain the control library and framework crosswalks.
- Identify overlapping requirements across frameworks and customer commitments.
- Keep control documentation current as the environment changes.

CONTROL ASSESSMENT AND EVIDENCE

Assess controls against applicable frameworks and collect the evidence needed to demonstrate they operate effectively.

- Perform periodic control self-assessments.
- Collect and organize audit evidence and artifacts.
- Track control ownership and testing cadence.
- Identify and log control gaps and deficiencies.

AUDIT AND CERTIFICATION SUPPORT

Coordinate SOC 2, ISO 27001, and similar audits and certifications. Prepare evidence packages, manage auditor requests, and track findings through remediation.

GAP AND REMEDIATION TRACKING

- Maintain a register of control gaps and remediation actions.
- Work with control owners to close deficiencies.
- Report on remediation progress and residual risk.

POLICY AND DOCUMENTATION

Support the maintenance of security policies, standards, and procedures, and confirm they align to the frameworks the organization commits to.

CUSTOMER AND VENDOR ASSURANCE

Respond to customer security questionnaires and support vendor and audit inquiries with accurate control information.

REQUIRED QUALIFICATIONS

- Bachelor's degree in Information Systems, Cybersecurity, or a related discipline, or equivalent experience.
- 2 to 5 years of experience in security compliance, GRC, IT audit, or information security.
- Working knowledge of common security frameworks and control concepts.
- Experience collecting audit evidence and supporting certifications.

- Strong documentation, organization, and communication skills.
- Ability to work across security, IT, and business teams.

PREFERRED CERTIFICATIONS

One or more of: CompTIA Security+, CISA, CRISC, ISO 27001 Lead Auditor or Lead Implementer, or equivalent.

TECHNICAL KNOWLEDGE

Security control assessment, framework mapping and crosswalks, evidence collection, audit and certification support, gap and remediation tracking, security policy documentation, customer security questionnaires, and GRC platforms.
