Job Title: Senior Technical Compliance Program Manager

Location: Remote or Colorado

Employment Type: Full Time

About Us

QI Path's software team is a group of technically sharp, humble developers focused on building high-quality software. Our SaaS and on-premises software is critical to identifying, managing and mitigating risk in medical and military communities where the stakes are high and lives are on the line. Collaboration, craftsmanship, and continual improvement are core to how we work. We encourage challenging the status quo and exploring novel ideas to solve our client's unique challenges. If you thrive on being a part of a team that transforms concepts into polished, functional web experiences—and love working with a team that values both technical excellence and friendliness—you'll fit right in.

The Role

QI Path is seeking an experienced Senior Technical Compliance Program Manager to lead and coordinate the technical and regulatory compliance activities associated with our software products and government customer deployments.

This role combines federal compliance expertise, technical understanding, and strong program management skills. The ideal candidate understands complex security and regulatory requirements, can translate them into actionable work, and is comfortable

working across engineering teams, company leadership, government stakeholders, and external assessors.

We are looking for someone who can take ownership of compliance initiatives from initial requirements analysis through documentation, implementation coordination, assessment, and completion.

This is not primarily a software development or hands-on engineering position. However, a strong technical foundation and the ability to work effectively with engineering and infrastructure teams are essential.

Key Responsibilities

Federal Compliance & Authorization

- Lead and coordinate compliance activities associated with federal government software deployments, including Authorization to Operate (ATO) and Risk Management Framework (RMF) processes.
- Interpret and manage applicable requirements from NIST 800-53, DISA STIGs including Application Security and Development, secure PII and PHI handling, and other relevant federal security frameworks and standards.
- Identify, research, and clarify regulatory, contractual, and customer-specific compliance requirements.
- Coordinate security assessments, vulnerability findings, remediation activities, and supporting evidence.
- Work with government security representatives, assessors, and other stakeholders throughout authorization and compliance processes.
- Help establish repeatable approaches to compliance across products and customer environments.

Compliance Documentation & Evidence

- Personally develop, maintain, and coordinate compliance documentation, including System Security Plans (SSPs), Plans of Action and Milestones (POA&Ms), security control narratives, and supporting artifacts.
- Coordinate the collection and validation of technical evidence from engineering, infrastructure, and security personnel.
- Maintain accurate records of compliance requirements, control implementation status, findings, risks, and remediation progress.
- Ensure documentation is organized, current, and prepared for customer reviews, assessments, and audits.

Program & Project Management

- Own compliance-related projects and initiatives, including planning, scheduling, tracking, and delivery.
- Translate compliance requirements into clear tasks and deliverables for the appropriate teams.
- Coordinate work across engineering, infrastructure, IT security, leadership, and external stakeholders.
- Identify dependencies, risks, and potential delays, and proactively drive resolution.
- Provide clear, concise status updates to leadership and customers.
- Establish and improve processes for tracking compliance obligations and maintaining ongoing readiness.

Technical Coordination

- Work closely with engineering and infrastructure teams to understand system architectures, configurations, security controls, and technical constraints.
- Coordinate STIG assessments and remediation, vulnerability management activities, and implementation of required security controls.

- Help determine responsibility for compliance requirements across application software, infrastructure, hosting environments, and customer-managed systems.
- Review technical findings and documentation for completeness and alignment with applicable requirements.
- Serve as a bridge between compliance stakeholders and technical teams.

Collaboration & Continuous Improvement

- Serve as a knowledgeable point of contact for compliance-related discussions with government customers and external partners.
- Collaborate with QI Path's IT Security Manager to ensure alignment between product-related compliance and corporate security initiatives.
- Help identify emerging or previously unrecognized compliance obligations.
- Recommend improvements to compliance processes, documentation practices, and internal coordination.
- Support the future development of a broader compliance function as organizational needs grow.

Required Qualifications

- 7+ years of relevant experience in federal cybersecurity compliance, security authorization, technical compliance, or related program management roles.
- Demonstrated experience with federal ATO/RMF processes, including preparation or coordination of authorization documentation and supporting evidence.
- Strong working knowledge of NIST security frameworks, particularly NIST SP 800-53.
- Familiarity with DISA STIGs, security assessments, vulnerability remediation, and compliance tracking.
- Experience personally preparing and maintaining compliance artifacts such as SSPs, POA&Ms, and security control documentation.

- Strong program and project management skills, including the ability to independently organize and drive complex, cross-functional initiatives.
- Sufficient technical understanding to work effectively with software engineers, infrastructure personnel, and security professionals.
- Excellent written and verbal communication skills, including the ability to explain complex technical or regulatory requirements to different audiences.
- Ability to work independently, manage competing priorities, and bring structure to ambiguous or evolving requirements.
- Must be eligible to obtain and maintain a DoD Common Access Card (CAC), subject to applicable government sponsorship and eligibility requirements.

Preferred Qualifications

- Direct experience supporting DoD software systems, deployments, or authorization processes.
- Experience working with government Authorizing Officials, ISSMs, ISSOs, security assessors, and related stakeholders.
- Prior or current DoD CAC issuance and familiarity with DoD onboarding and access processes.
- Experience supporting multiple ATO efforts or managing compliance across multiple systems.
- Familiarity with government-hosted, on-premises, and cloud-based software environments.
- Experience working with commercial software vendors serving federal government customers.
- Familiarity with FedRAMP, NIST SP 800-171, CMMC, or other applicable compliance frameworks.
- Relevant certifications such as CISSP, CGRC, CISM, or PMP.

What Success Looks Like

The successful candidate will bring clarity, organization, and accountability to QI Path's technical compliance activities.

They will be able to independently assess requirements, identify gaps, establish actionable plans, coordinate the necessary people and resources, and drive initiatives through completion.

They will also be comfortable personally developing required documentation while working with technical teams to ensure compliance obligations are properly understood and addressed.

Most importantly, this person will become a trusted resource for engineering, leadership, and government stakeholders, helping QI Path navigate complex compliance requirements efficiently and confidently.

What We Offer

- A life protecting mission: When we do our job well, lives are saved — for our country’s front-line medical and military workers, and for the safe development of new medicine.
- A team that values humility, expertise, and helping each other grow
- Remote-friendly work environment
- We strive to provide a healthy work-life balance so you can keep energized and focused on the mission
- Opportunities to expand your skills across the stack
- Paid time off
- Medical benefits with employer contribution