

Guiding Rizkly to FedRAMP High Authorization

A SecureIT Advisory Case Study

Rizkly, a cloud-based compliance automation provider, engaged SecureIT to provide full lifecycle **FedRAMP High Advisory services**, supporting the company's successful journey toward achieving a **FedRAMP High Authorization to Operate (ATO)**.

As a **FedRAMP Third-Party Assessment Organization (3PAO)** and trusted cybersecurity advisor, SecureIT applied its structured FedRAMP methodology refined through years of experience with high-impact systems to guide Rizkly from early gap assessment through documentation development, remediation, and pre-assessment readiness.

Throughout the engagement, SecureIT combined expert advisory support with modern automation and AI-enabled efficiencies to streamline document generation, validation, and control evidence tracking – enabling Rizkly to progress efficiently while maintaining the rigor required for High Baseline compliance.

A Three-Phased Approach



Phase 1:
**FedRAMP High Gap
Assessment**



Phase 2:
**Documentation
Development**



Phase 3:
**Gap Remediation
and Pre-Assessment
Readiness**

The Process

Phase 1: FedRAMP High Gap Assessment

SecureIT began by performing a comprehensive **FedRAMP High Gap Assessment** based on the **NIST 800-53 Rev. 5 High Baseline** and all FedRAMP-defined control parameters.

Working closely with Rizkly's technical and compliance teams, SecureIT conducted detailed documentation reviews and structured interviews covering system architecture, data flows, encryption practices, access controls, incident response, and continuous monitoring processes.

This phase identified specific control deficiencies and boundary considerations and resulted in a **risk-rated Plan of Action and Milestones (POA&M)**. The POA&M provided a clear, prioritized roadmap for Rizkly's remediation efforts and served as the foundation for future documentation and implementation work.

SecureIT's structured analysis helped Rizkly's team fully understand how each control applied to its environment and what technical and procedural steps were needed to meet FedRAMP High standards.

Phase 2: Documentation Development

Following the gap assessment, SecureIT led the development of Rizkly's **FedRAMP documentation package**, including the **System Security Plan (SSP)**, the controls not inherited by the FedRAMP authorized IaaS and PaaS providers, and more than 30 required appendices and policy artifacts.

These documents were created using **FedRAMP templates** and tailored to Rizkly's architecture, security tools, and operational practices. SecureIT facilitated working sessions with Rizkly's subject matter experts to gather details on configurations, network diagrams, encryption mechanisms, and access control procedures.

Where appropriate, automation and AI-assisted tools were incorporated to help populate standard control statements and verify internal consistency across the documentation set – supporting accuracy and accelerating delivery.

The result was a complete and FedRAMP-ready package, formatted and written to PMO standards, reflecting both the maturity of Rizkly's platform and its alignment with federal cloud security expectations.

Phase 3: Gap Remediation and Pre-Assessment Readiness

While documentation development was underway, Rizkly's teams executed the technical and procedural remediations identified in the POA&M. SecureIT provided **ongoing advisory support**, conducting targeted technical workshops and control validation sessions to help resolve complex implementation issues and confirm compliance with FedRAMP requirements.

As remediation decisions evolved – such as updates to monitoring tools, MFA integrations, or encryption configurations – SecureIT refreshed the relevant sections of the SSP and supporting appendices to ensure accuracy.

Before Rizkly was assessed by a 3PAO, SecureIT facilitated a **pre-assessment readiness review** to validate that all required evidence, configurations, and security controls were in place and functioning as expected. This proactive approach helped minimize findings during the formal assessment phase.

Results

Through this collaborative engagement, Rizkly achieved its **FedRAMP High Authorization**, demonstrating compliance with the most stringent federal security standards.

The engagement highlighted the effectiveness of SecureIT's proven FedRAMP methodology and its ability to adapt to each client's environment and tools. By leveraging automation selectively – including AI-enabled document validation and consistency checks – SecureIT and Rizkly maintained both precision and efficiency throughout the project lifecycle.

Key outcomes included:

- Completion of a fully compliant FedRAMP High documentation package
- Streamlined remediation and evidence gathering
- Successful readiness validation prior to 3PAO assessment
- FedRAMP High Authorization granted to Rizkly

Conclusion

End-to-End Compliance & Cybersecurity Solutions

The partnership between **Rizkly and SecureIT** demonstrates how experienced FedRAMP advisors can accelerate compliance readiness for innovative cloud providers. By combining expert advisory support, deep understanding of federal security frameworks, and modern documentation tools, SecureIT helped Rizkly reach one of the highest benchmarks in cloud security compliance – **FedRAMP High Authorization**.

This engagement reflects SecureIT's continued commitment to helping technology providers achieve authorization efficiently, accurately, and sustainably – enabling them to deliver secure, trusted solutions to U.S. federal agencies.

Ready to simplify cybersecurity and compliance for your organization?

Contact SecureIT to schedule a consultation and let us tailor a solution for your environment.



Visit us

12110 Sunset Hills Road, Suite
600, Reston, VA USA 20190

Email us

info@secureit.com

Call us

703 464-7010

