FEDRAMP READINESS & GAP ASSESSMENT SERVICES

Accelerate Your Path to FedRAMP Authorization

Federal agencies require cloud service providers to achieve a **FedRAMP Authorization to Operate** (**ATO**). Getting there is complex — you must align with hundreds of NIST SP 800-53 security controls, develop a **System Security Plan** (**SSP**), and pass an independent **Third-Party Assessment Organization** (**3PAO**) audit.

Koniag Cyber helps organizations **prepare confidently and avoid costly delays** by providing **FedRAMP Gap Assessments & Readiness Services.**

Our Approach

01

Discovery & Environment Mapping

We review your architecture, boundary definitions, and inherited controls to understand your cloud service and operating model.

02

Gap Analysis Against FedRAMP Baseline

We review your architecture, boundary definitions, and inherited controls to understand your cloud service and operating model.

03

Remediation Roadmap

We deliver a prioritized Plan of Action & Milestones (POA&M) with actionable steps to close gaps before engaging a 3PAO.

04

Documentation & Package Preparation

We help draft and refine required artifacts — SSP, Security Assessment Plan (SAP), Policies & Procedures, Inventory, Control Evidence.

05

Pre-Assessment Validation

Optionally, we conduct a readiness review simulating a 3PAO audit to validate closure of gaps.

Why Choose the Koniag Team

Proven FedRAMP & NIST Expertise

Specialists in **NIST SP 800-53, FedRAMP SAF, and cloud security.**

Authorized Assessor Alignment

We partner with **FedRAMP-accredited Third-Party Assessment Organizations (3PAOs)** so our readiness work mirrors the exact approach an official assessor will take.

End-to-End Support

From discovery to documentation and remediation guidance.

Trusted Heritage

Part of the **Koniag family of companies**, a 50-year legacy of trusted government and commercial partnerships.

Local & Flexible Delivery

Remote support with the ability to place experienced resources on-site as needed.

Integrated Cybersecurity Services

Beyond readiness: continuous monitoring, incident response, and managed detection & response (MDR).

Typical Engagement Deliverables

- **Gap Analysis Report** (control-by-control scoring)
- **POA&M/Remediation Roadmap** with risk & effort ranking
- **Draft FedRAMP SSP** and supporting documentation
- **Pre-Assessment Audit Findings & Recommendations**
- **Executive Readout** for leadership & stakeholders

We help our clients be foundationally prepared and ahead of next-generation threats

Let's get started at:
koniagcyber.com/contact
info@koniagcyber.com