FedRAMP Preparatory Procedures

Achieving a FedRAMP ATO is challenging, even for the most prepared team. In addition to being an accredited Third-Party Assessor Organization (3PAO), MindPoint Group provides several preparatory services to scale you into FedRAMP efficiently and in a cost-effective manner.

Critical Controls Assessment

- Confirms FIPS 199 System Categorization
- In depth review of 20 critical FedRAMP Controls
- Perform a high-level documentation review to highlight critical elements missing from the documents
- Stake holder interviews related to the 20 critical FedRAMP controls reviewed
- Review of the ATO boundary and network and data flow Diagrams
- Report provided to customers with a general understanding of their FedRAMP readiness and areas for improvement

Gap Assessment

- Confirms FIPS 199 System Categorization
- Reviews all the FedRAMP controls applicable to the system categorization and rates in order of criticality
- Stake holder interviews to understand the cybersecurity posture of the system in more detail and determine where documentation doesn't accurately reflect current processes
- Full review of all security documents currently generated and analysis of what is missing or non-complaint
- Review of ATO Boundary, Network and Data flow diagrams
- Report provided to customer with a general understanding of their FedRAMP readiness and areas for improvement

No matter the service you choose, MindPoint Group's methodology is focused on providing informative, helpful engagements that maximize your understanding and benefit from FedRAMP compliance.

VISIT US www.mindpointgroup.com **EMAIL** info@mindpointgroup.com

MindPoint GROUP℠

What activities can we expect with each offering?

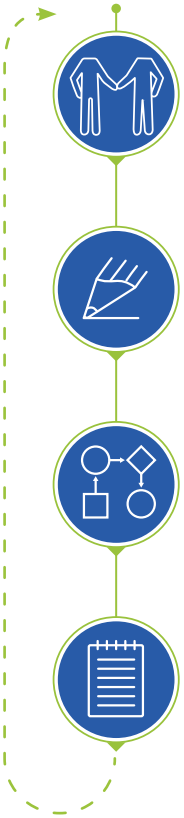
Task	Critical Controls Assessment	Gap Assessment
Documentation Review	✓	✓
Interviews	✓	✓
Evidence Gathering	✗	✗
Technical Testing	✗	✗
Penetration Testing	✗	✗
FedRAMP Required Templates for Reporting	✗	✗
3-Year Testing Strategy	✗	✗
Controls Assessed	40	Full for system categorization

Methodology

PLANNING

Many FedRAMP projects miss important deadlines and go over budget because of inefficient planning. Without knowing what to expect, it can feel like you're greatly underprepared. We understand that you're new to this process, so we'll spend all the time necessary beforehand to establish clear timelines, testing procedures, project milestones, budgeting, and responsibilities. Effective planning layers in several key elements:

1. The Assessment Team
2. Scope
3. Approach
4. Deliverables



Assessment Team

- Meet your dedicated assessors
- Meet your project Manager

Scope

- Confirmations of System Categorization
- Applicable Controls Identified

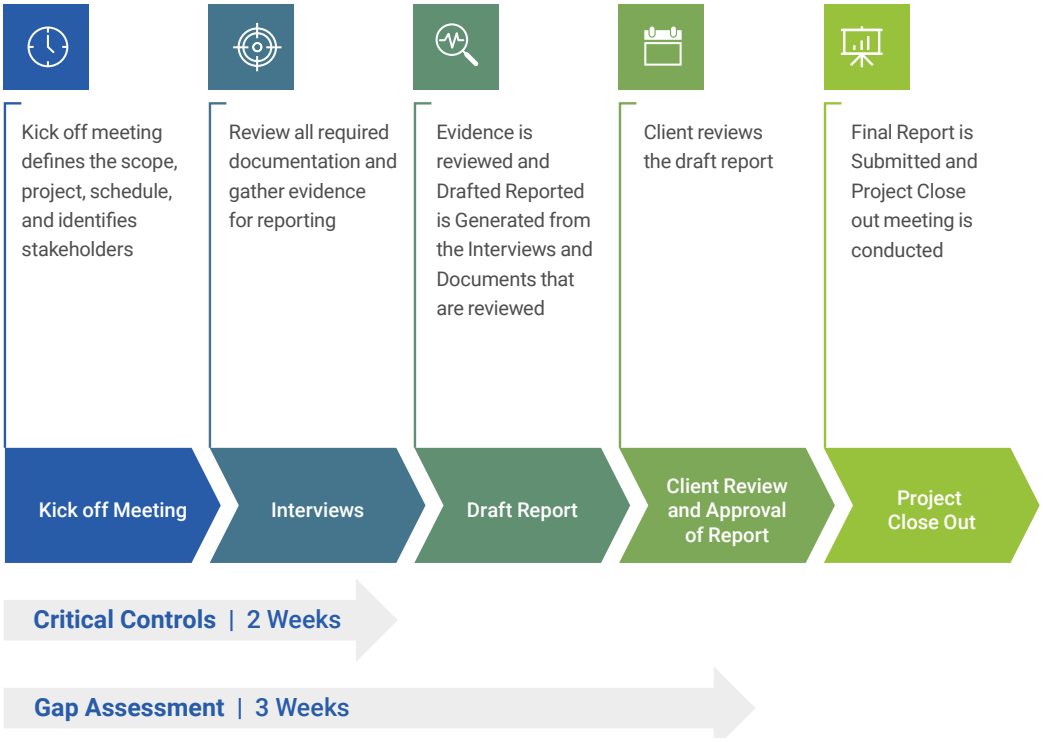
Approach

- Proposed Assessment Schedule
- Document Sharing

Deliverables

- Assessment Report identifying gaps and general recommendations for remediation

MPG will meet with you and any other stakeholders to discuss the assessment engagement before finalizing an agreed-upon schedule. Our assessment team is supported by Project and Account Managers who will be on hand to assist in making sure the assessment procedures run smoothly, and timelines are met. As part of the planning process, MPG will provide an agenda and other key assessment components for the assessment.



ASSESSMENT

MPG conducts Preparatory Assessments using the NIST 800-53 Revision 4 Risk Management Framework and the FedRAMP-mandated overlay controls. We follow similar procedures for each type of assessment we do, but some take more time than others, depending on the level of granularity and number of controls the assessment requires.

Please note that unlike official 3PAO Assessments, MPG does not utilize technical testing and observational evidence from customers during a Critical Controls and Gap Assessment. Stakeholder interviews and an exhaustive documentation review will provide enough information on a system's cybersecurity posture to cite findings and suggest remediation actions. Then, during the 3PAO assessment, remediations suggested during the initial analysis can be evidenced through observation and testing procedures required of a 3PAO assessment.

TASKS

Documentation Review

MindPoint Group will review the associated security documentation submitted by the Customer. Policies, procedures, diagrams, and supporting evidence should be provided to ensure that MindPoint Group can effectively evaluate the security control implementation status and effectiveness. Any control that cannot be adequately assessed with the evidence, testing, and interviews, will be documented as such within the Gap Assessment Draft Report or the official Security Assessment Report.

MPG will analyze some, if not all, of the following policies and procedures during an assessment:

- System Security Plan and the following attachments
- E-Authentication Plan
- Privacy Threshold Analysis (PTA) / Privacy Impact Assessment (PIA)
- Rules of Behavior
- Information System Contingency Plan (ISCP)
- Configuration Management Plan (CMP)
- Incident Response Plan (IRP)
- Control Implementation Summary (CIS) Workbook
- Laws and Regulations
- Information System Security Policies & Procedures mapping to the 17 NIST control families
- Continuous Monitoring Plan (ConMon Plan)

Interviews

MPG will conduct interviews with a variety of customer stakeholders ranging from sysadmins through to head of operations. The exercise is intended to better understand the processes followed during day-to-day operations as they relate to security. The interview process is critical to the success of this phase because understanding the service offering, the associated business processes, and the security controls allows for the development of effective and efficient test procedures.

Reporting

Upon completion of the assessment, the team will document and report assessment results, findings, and associated risks. MPG will submit the report in draft form to key stakeholders involved with the project for review and comment prior to being finalized and formally delivered. MPG's project close-out meeting will be a venue for summarizing the findings and associated risks captured in the report and providing completed deliverables.