Datasheet

FedRAMP Assessment Procedures

Achieving a FedRAMP ATO is challenging, even for the most prepared team. In addition to being an accredited Third-Party Assessment Organization (3PAO), MindPoint Group provides accredited FedRAMP assessment services to meet your current assessment needs.

Critical Controls Assessment

- Confirm FIPS 199 System categorization
- Review controls outlined by FedRAMP for a FedRAMP Readiness Assessment
- Stake holder interviews to understand the cybersecurity posture of the system in more detail and determine where documentation doesn’t accurately reflects current processes
- Full review of all security documents currently generated and analysis of what is missing or non-compliant
- Report provided to customer utilizing FedRAMP Readiness Report Template

Gap Assessment

- Facilitate security controls requirements gathering from the Authorizing Official (AO) or representative
- Develop and gaining approval for Security Assessment Plain (SAP) utilizing the FedRAMP Template
- Gather existing security documentation and performing a detailed evaluation
- Conduct necessary testing in conjunction with interviews for certain controls utilizing shoulder surging or other comparable techniques
- Performing an initial vulnerability scan and penetration test
- Assessing control implementation and effectiveness and documenting identified vulnerabilities and associated risk utilizing the FedRAMP Security Assessment Report
- Post-assessment submission to PMO

3PAO Assessment

- Facilitate security controls requirements gathering from the Authorizing Official (AO) or representative
- Develop a 3-year testing strategy for continuous monitoring assessment
- Develop and gaining approval for a Security Assessment Plan (SAP) utilizing the FedRAMP Template
- Gather existing security documentation and performing a detailed devaluation
- Conduct interviews with key stakeholders
- Conduct necessary testing in conjunction with interviews for certain controls utilizing shoulder surfing or other comparable techniques
- Performing an initial vulnerability scan and penetration test
- Assessing control implementation and effectiveness and documenting identified vulnerabilities and associated risk utilizing the FedRAMP Security Assessment Report
- Post-assessment submission to PMO

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?

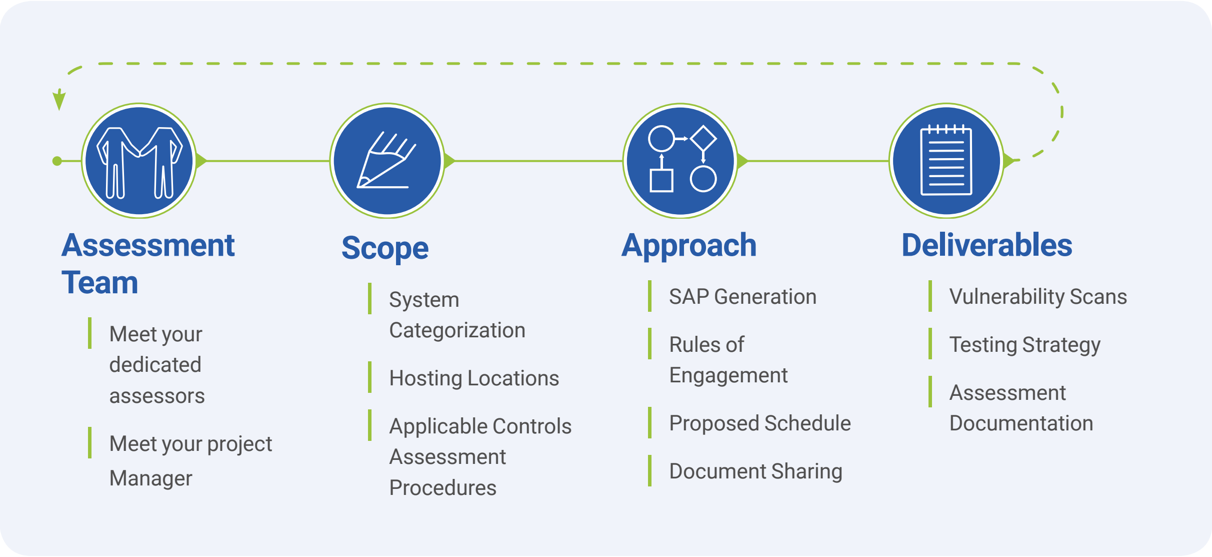
Task	FedRAMP Readiness Assessment	3PAO Assessment	Continuous Monitoring Assessment
Documentation Review	✓	✓	✓
Interviews	✓	✓	✓
Evidence Gathering	Partial	✓	✓
Technical Testing	✕	✓	✓
Penetration Testing	✕	✓	✓
FedRAMP required templates for reporting	✓	✓	✓
3-year testing strategy	✕	✕	✓
Controls assessed	Based on FedRAMP Readiness Assessment Requirements template	Full for system categorization	Per FedRAMP common requirements (e.g. moderate is between 175-180)

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

- System Categorization
- Hosting Locations
- Applicable Controls Assessment Procedures

Approach

- SAP Generation
- Rules of Engagement
- Proposed Schedule
- Document Sharing

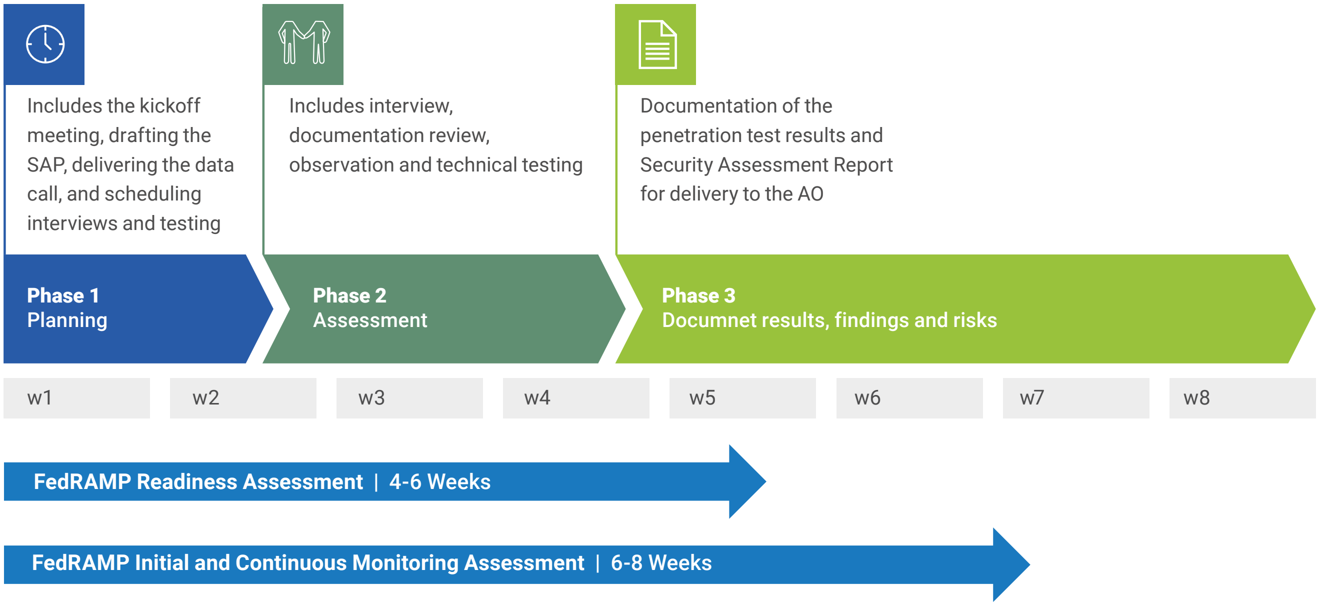
Deliverables

- Vulnerability Scans
- Testing Strategy
- Assessment Documentation

MindPoint will meet with you, the Authorizing Official (AO), and any other stakeholders to discuss the test engagement prior to 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 a Security Assessment Plan (SAP) that details the methodology, control selection, agenda, and other key assessment components for the assessment utilizing the standardized SAP template.

ASSESSMENT

MPG conducts FedRAMP 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.



Includes the kickoff meeting, drafting the SAP, delivering the data call, and scheduling interviews and testing

Phase 1
Planning

Includes interview, documentation review, observation and technical testing

Phase 2
Assessment

Documentation of the penetration test results and Security Assessment Report for delivery to the AO

Phase 3
Documnet results, findings and risks

w1	w2	w3	w4	w5	w6	w7	w8

FedRAMP Readiness Assessment | 4-6 Weeks

FedRAMP Initial and Continuous Monitoring Assessment | 6-8 Weeks

Please note that unlike official 3PAO assessments, MPG does not require technical testing and observational evidence from customers during a Critical Controls and Gap Analysis. 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 Analysis Draft Report or the official Security Assessment Report.

Some, if not all, of the following policies and procedures will be analyzed by MPG 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

MindPoint Group will conduct interviews with a variety of customer stakeholders ranging from sysadmins through to Head of Operations. The exercise is intended to get a better understanding of 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.

OBSERVATION

During official 3PAO assessments, MindPoint Group may need to physically observe security controls and processes as they are performed by customer personnel and/or systems. In these cases, support personnel with the knowledge and access to demonstrate security control functionality should be made available.

TESTING

Official 3PAO assessments require technical testing against documented controls. Technical testing may require population sampling and the gathering of associated artifacts to support control implementation statements. The information gathered through these processes will be used to document security control effectiveness and to identify control deviations for the cloud service offering. Technical testing will also include a vulnerability scan and penetration test, in compliance with FedRAMP Penetration Testing Guidance document.

REPORTING

Upon completion of the assessment, the team will document and report assessment results, findings, and associated risks using a standardized Security Assessment Report (SAR). MindPoint Group 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. MindPoint Group's project close-out meeting will be a venue for summarizing the findings and associated risks captured in the report and providing completed deliverables.

For more information

VISIT US mindpointgroup.com/service-areas/fedramp-3pao-services/
EMAIL info@mindpointgroup.com

MindPoint GROUP℠