Post Authorization: Continuous Monitoring

THE FEDRAMP APPROACH: Continuous Monitoring for Agency ATOs and JAB P-ATOs

Each CSP

- Maintains inventory through change management process
- Ensures scanning tools appropriately target the correct assets
- Runs security scans at least monthly: OS, DB, and Webserver
- Tracks findings and remediation in the POA&M on an ongoing basis
- Submits a snapshot of their POA&M and inventory monthly, along with Web, OS, and DB scans

To FedRAMP for P-ATO

Each CSP Delivers:
- Scanner Output (Web, DB, OS)
- Asset Inventory
- POA&M

To Agency AOs for FedRAMP Agency ATO

FedRAMP ConMon Team

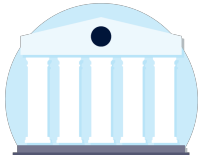
- Processes and correlates each CSP's Scans, Inventory, & POA&M
- Aggregates and trends against past submissions
- Identifies metrics that exceed non-compliance thresholds
- Produce Draft ConMon Report

Agency AO Representatives

- Manually correlate each CSP's Scans, Inventory, and POA&M
- Look for non-compliance
- Look for changes in risk posture
- Report summary concerns to AO

JAB Review Team

- Investigates anomalies and non-compliance flags
- Validates and updates ConMon Report
- Approves ConMon Report
- Publishes to leveraging Agencies



Leveraging Agencies

JAB P-ATO
Continuous Monitoring

JAB CONTINUOUS MONITORING AT A GLANCE

30+ JAB authorizations:

- Leveraged for over 200 authorizations
- by over 45 Agencies
- ~5 Million Assets

For every JAB-authorized system we:

- Analyze, correlate, track, and trend scanner tool output and POA&M submissions monthly
- Track, review, and adjudicate 20-40 Significant Changes and 1,600 Deviation Requests per year
- Track, review, and adjudicate Annual Assessment packages

We achieve this with:

- A dedicated team of experienced people
- Proven, and continuously improving processes; and
- Mature automation capabilities

Agency ATO
Continuous Monitoring

CONTINUOUS MONITORING
Agency Overview

Continuous Monitoring ensures a service offering maintains an appropriate security posture for the life of the system at an Agency

CSPs maintain and validate the security posture of their service offering through:

- Vulnerability Management
  - Monthly OS / Web / Database raw scans
  - POA&M & Updated Inventory
  - Configuration Management / System Changes
- Annual Assessment of the Service Offering
- Incident Reporting

Highlights of Agency ConMon:

- ConMon deliverables are the same for any CSP that is FedRAMP Authorized (JAB or Agency)
- All ConMon deliverables are required to be posted to OMB MAX by the CSP
- Each Agency should perform their own review of these deliverables

CONTINUOUS MONITORING
Requirements for Agencies and CSPs

CSP REQUIREMENTS

- Submit monthly POA&M, monthly database, OS, inventory files, and web application raw scan files
- Submit Deviation Requests and Significant Change Requests as necessary
- If an incident occurs, the CSP should adhere to US-CERT guidelines
- Submit annual assessments to FedRAMP
- Respond to Agency questions and concerns and remediate vulnerabilities as required in the agreed upon timeframe
- Adhere to the continuous monitoring plan defined in the CSP's SSP (re: CA-7)

AGENCY REQUIREMENTS

- Review monthly and annual ConMon materials and ensure they agree with any changes, deviation requests, scans, etc. and that the risk posture is acceptable
- Provide feedback to the CSP if you have questions or concerns regarding any of the ConMon deliverables / security posture
- Reach out to the FedRAMP PMO at info@fedramp.gov with any questions regarding specific continuous monitoring vulnerabilities or if you are unable to obtain the information you need.

VULNERABILITY MANAGEMENT
Requirements & Best Practices

CSP REQUIREMENTS

- Authenticated Scans
- Complete System Scans*
- Remediations are Completed in Required Timeframes from Date of Discovery
- Understand Vendor Dependencies

** If complete system scanning is not possible, CSPs should consider employing strategic sampling*

Best Practices

- Every Agency should perform ConMon
- CSPs should use the same method, where practical, to show resolution
- Deviation Requirements (DRs):
  - Operational Requirements (ORs)
  - False Positives (FPs)
  - Risk Adjustments (RAs)
- Establish / Utilize Multi-Agency ConMon Collaborative groups where available

FEDRAMP REMEDIATION TIMEFRAMES

High	Moderate	Low
30 Days	90 Days	180 Days

VULNERABILITY MANAGEMENT
Monthly Requirements

CSPs are required to submit the following to their Agency customer(s) on a monthly basis:

DELIVERABLE	DELIVERABLE REQUIREMENTS
Monthly POA&M	• Complete inventory of new, open, and close POA&M items • Consistent versioning among POA&Ms
Raw Scan Files	• Authenticated scan files • Original OS / Web / DB Scans • Complete asset inventory
Deviation Requests (DR)	• System deviations should be communicated to the Agency AO using the FedRAMP DR Form
Significant Change Requests (SCR)	• System deviations may be considered significant by the CSP or Agency customer • SCRs should be submitted using the FedRAMP SCR Form

CONFIGURATION MANAGEMENT
Significant Changes

Significant Change Process

Identify and Communicate a Significant Change
If a CSP believes a change to the service offering is significant, they are required to vet the change to all Agency AOs via a Significant Change Request (SCR)

CSPs Engage a 3PAO to Plan for Assessment
Following AO approval of the change, the CSP should engage a 3PAO to develop an assessment plan and provide to the Agency AO for review and approval prior to testing

CSP Implements Change & 3PAO Assesses
Once the AO approves the assessment approach, the 3PAO and CSP should commence testing and provide the results (SAR) to all Agency AOs.

Agency AO reviews the updated assessment report and authorizes changes
The 3PAO should present an updated SAR to the AO for review and validation that the security posture of the system remains acceptable for the system following the change.

Identifying a significant change:

- Security impact analysis for the change
- AO / CSP engage to understand the change

Pre-approval of a significant change:

- CSP should work with their 3PAO prior to submitting a SCR
- The CSP should not proceed without clear direction from the AO
- SCRs can either be:
  - Tested when submitted
  - Tested during Annual Assessment (must be included in SAP)

Types of significant changes:

- Authentication / Access Control
- Change in FIPS 199 Status
- Change in SaaS / PaaS underlying provider
- Removal of security controls
- Implementation of mitigating / alternate controls
- Change in system scope
- Replacement of COTS product

ANNUAL ASSESSMENT

Annual Assessments are required to re-validate a
cloud service offering's security posture for the life of the system

REQUIREMENTS:

- Annual Assessments must be completed annually, beginning 1 year after the initial ATO letter is signed
- Each annual assessment covers 1/3 of the implemented controls, including a set of critical controls
  - This ensures that - over 3 years - all controls in a system are re-tested
- CSPs must prepare updated documentation for each annual assessment
- CSPs must engage a 3PAO to complete annual assessment testing
- Annual Assessments should validate that:
  - Closed POA&M items are indeed closed
  - Deviation Requests and impacted controls are reconciled
  - Assessments for significant controls outside of the annual assessment window did not impact the risk posture

ANNUAL ASSESSMENTS
Approach / Review Strategy

CSPs must prepare the following deliverables, annually, for all agencies that have issued an ATO for a given CSO:

DELIVERABLE	DELIVERABLE REQUIREMENTS
SAP	• The SAP provides the scope of testing for the annual assessment. • Each annual assessment covers a different third of the controls, so that over a period of three years, all controls are re-tested. The SAP should clearly define the scope for this.
SSP / Scope / Core Controls / AO Prescribed	• The SSP is a living document and should be updated as changes are made to the system. CSPs should provide the most updated SSP to agencies as part of the annual assessment for the opportunity to formally re-review any changes that have been made.
SAR	• Once testing is complete, the 3PAO will produce a SAR for the Agency to review. The SAR will convey all vulnerabilities / deficiencies identified during testing.
POA&M	• In addition to the SAR, the 3PAO, CSP, and Agency should collaborate on the development of a POA&M to ensure that vulnerabilities are mitigated within FedRAMP's defined timeframes. • The Clock starts as soon as a CSP is aware of vulnerability / weakness.

Please refer to the Continuous Monitoring Strategy Guide on FedRAMP.gov for more information about annual assessments.

INCIDENT MANAGEMENT
Requirements & Best Practices

US CERT reporting requirements are non-negotiable

- Agencies must report information security incidents to the NCCIC / US-CERT within one hour of being identified

The Incident Response Plan defines additional reporting roles and responsibilities for each system and Agency

- Maintaining accurate POC information is critical
- Agencies must monitor Agency-configured portion of system
- Agencies and CSPs must notify each other based on who becomes aware of an incident first

FedRAMP or individual Agency AOs may direct the CSP to treat certain critical vulnerabilities as incidents, such as "zero day" vulnerabilities (e.g. Heartbleed)