**FedRAMP 20x, Community Working Group- Rev 5 Continuous Monitoring**

**Proposal Submitter: Sai Sravan Cherukuri, FedRAMP recognized 3PAO assessment team member, 03-27-2025**

**Standard for Continuous Monitoring Reporting by Cloud Service Providers (CSPs) under FedRAMP Rev 5 and Legacy Rev 4**

# 1.Introduction

Continuous Monitoring (ConMon) is a cornerstone of FedRAMP, ensuring that authorized Cloud Service Offerings (CSOs) maintain a **resilient and transparent security posture**. This standard establishes a **structured, automated, and risk-driven reporting framework**, equipping **agency security professionals** with real-time security insights.

By defining **specific reporting templates, compliance checklists, and an API schema for automated report ingestion**, this standard **elevates ConMon beyond a compliance requirement,** it **optimizes security visibility, automates risk assessment, and enhances proactive threat mitigation**.

**2.Purpose**

The purpose of this standard is to ensure that CSPs with both FedRAMP Revision 5 (Rev 5) and legacy FedRAMP Revision 4 (Rev 4) authorizations provide security professionals across federal agencies with reliable, consistent, and actionable insights into the security posture of their Cloud Service Offering (CSO).

# 3. Scope and Applicability

This standard applies to all CSPs that maintain a FedRAMP authorization at any impact level (Low, Moderate, or High). It outlines the minimum requirements for continuous monitoring reporting to ensure transparency, risk validation, and compliance with evolving cybersecurity threats.

# 4. Objectives

* Establish a uniform ConMon reporting format that aligns with FedRAMP Rev 5 controls and accommodates legacy Rev 4 systems.
* Provide agency security professionals with timely, accurate, and meaningful risk insights into CSP environments.
* Ensure seamless integration of ConMon data into federal risk management frameworks and Security Operations Centers (SOCs).
* Enhance automation in reporting to reduce manual overhead and improve data accuracy.

# 5. Key Requirements for Continuous Monitoring Reporting

**5.1 Reporting Frequency and Submission**

* **Monthly POA&M Reporting:** CSPs must submit a Plan of Action & Milestones (POA&M) report monthly, detailing open, closed, and mitigated vulnerabilities.
* **Quarterly Vulnerability Scanning Reports:** Results from authenticated scans of operating systems, databases, and web applications must be submitted every quarter.
* **Annual Assessment Report:** A full reassessment of security controls must be conducted and submitted annually to ensure compliance with the system security plan (SSP).
* **Immediate Incident Reporting:** Any significant security incidents, breaches, or compromises must be reported within 60 minutes, followed by a detailed impact assessment within 24 hours.

**5.2 Security Control Performance Metrics**

CSPs must report on the following key metrics to demonstrate adherence to FedRAMP Rev 5 requirements:

* **Patch Management Compliance:** Percentage of critical vulnerabilities patched within prescribed timelines (e.g., 15 days for critical, 30 days for high severity).
* **Endpoint Security Posture:** Percentage of systems with active endpoint detection and response (EDR) tools.
* **Access Control Monitoring:** Summary of privileged access changes and multi-factor authentication (MFA) compliance rates.
* **Log and Event Management:** Percentage of security logs ingested into a Security Information and Event Management (SIEM) system and retention compliance with FedRAMP requirements.

**5.3 Threat Intelligence and Risk Assessment**

* CSPs must provide periodic threat intelligence reports that identify emerging risks and indicators of compromise (IOCs) relevant to the cloud environment.
* Risk scoring methodologies should be applied to prioritize vulnerabilities based on exploitability, potential impact, and asset criticality.
* CSPs should demonstrate their ability to detect and respond to zero-day threats by integrating federal threat intelligence sources such as CISA’s Automated Indicator Sharing (AIS).

**5.4 Automation and Data Exchange Standards**

* CSPs must leverage machine-readable formats (e.g., STIX/TAXII, JSON, XML) for ConMon reporting to facilitate automated ingestion by agency security tools.
* APIs should be provided for real-time data sharing with agencies utilizing Continuous Diagnostics and Mitigation (CDM) programs.
* Reports should align with NIST 800-53 Rev 5 and be mapped to federal risk management frameworks such as FISMA and Zero Trust Architecture (ZTA).

**5.5 Compliance with Legacy FedRAMP Rev 4**

For CSPs still operating under FedRAMP Rev 4, the following considerations apply:

* CSPs must submit a migration plan to transition to Rev 5 by the deadline set by FedRAMP PMO.
* Any security gaps between Rev 4 and Rev 5 must be documented with compensating controls.
* ConMon reporting must follow the enhanced guidelines of Rev 5 where feasible, especially in vulnerability management and automated reporting.

# 6. Standardized Reporting Templates

**6.1 Plan of Action & Milestones (POAM) Monthly Report**

**Purpose:** Tracks open vulnerabilities, remediation progress, and compliance with required patching timelines.

**Template Format:**

| **POA&M ID** | **Vulnerability Name** | **Severity** | **Identified Date** | **Due Date** | **Mitigation Plan** | **Current Status** | **Expected Completion Date** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| POAM-001 | OpenSSH Privilege Escalation | High | 2025-03-01 | 2025-03-15 | Patch to OpenSSH v9.3 | In Progress | 2025-03-12 |
| POAM-002 | Outdated TLS Version | Critical | 2025-02-20 | 2025-03-06 | Upgrade to TLS 1.3 | Completed | 2025-02-28 |

**Value Addition:** This structured approach allows agencies to track risk reduction over time and measure CSP responsiveness to security vulnerabilities.

**6.2 Quarterly Vulnerability Scanning Report**

**Purpose:** Demonstrates the effectiveness of CSP vulnerability management through automated scanning results.

**Template Format:**

| **Scan Date** | **System Scanned** | **# of Critical Findings** | **# of High Findings** | **# of Medium Findings** | **Remediation Rate (%)** |
| --- | --- | --- | --- | --- | --- |
| 2025-03-01 | App Server Cluster | 5 | 12 | 30 | 85% |
| 2025-03-01 | Database Cluster | 2 | 8 | 25 | 90% |

**Value Addition:** Agencies can immediately assess a CSP’s ability to detect and remediate vulnerabilities, improving risk-based decision-making.

**6.3 Annual Security Control Assessment Report**

**Purpose:** Evaluates adherence to FedRAMP controls, ensuring ongoing security compliance.

**Template Format:**

| **Control Family** | **FedRAMP Control** | **Assessment Result** | **Remediation Plan** |
| --- | --- | --- | --- |
| Access Control | AC-2: Account Management | Pass | N/A |
| Audit & Accountability | AU-6: Audit Review | Partial | Implement SIEM alerting for critical logs |
| System & Communications | SC-12: Cryptographic Key Management | Fail | Migrate to FIPS 140-3 compliant HSM |

**Value Addition:** Provides a structured compliance snapshot, highlighting areas of improvement and tracking control maturity.

**6.4 Incident Reporting Template (60-Minute Notification & 24-Hour Follow-Up)**

**Purpose:** Ensures timely notification and follow-up reporting for security incidents impacting federal systems.

**Template Format:**

**Initial Incident Notification (Within 60 Minutes)**

* **Incident ID:** INC-20250315-001
* **Date/Time Detected:** 2025-03-15 12:45 UTC
* **Incident Type:** Unauthorized Access
* **Affected System(s):** GovCloud East – Database Cluster
* **Impact Level:** High
* **Initial Mitigation Action:** Account Lockdown, SIEM Investigation Initiated

**Follow-Up Incident Report (Within 24 Hours)**

* **Root Cause Analysis:** Compromised credentials due to phishing attack.
* **Resolution Steps:**
  + MFA enforcement strengthened.
  + Privileged access review conducted.
* **Lessons Learned:** Additional employee phishing awareness training required.

**Value Addition:** Provides agencies with immediate situational awareness while enabling long-term security improvements.

**7. Standardized Reporting Templates**

**7.1 Plan of Action & Milestones (POAM) Monthly Report**

**Purpose:** Tracks open vulnerabilities, remediation progress, and SLA adherence.

**Structured Template**

{

"reporting\_period": "2025-03",

"csp\_name": "SecureCloudGov",

"findings": [

{

"poam\_id": "POAM-001",

"vulnerability\_name": "OpenSSH Privilege Escalation",

"severity": "High",

"identified\_date": "2025-03-01",

"due\_date": "2025-03-15",

"mitigation\_plan": "Patch to OpenSSH v9.3",

"status": "In Progress",

"expected\_completion\_date": "2025-03-12"

},

{

"poam\_id": "POAM-002",

"vulnerability\_name": "Outdated TLS Version",

"severity": "Critical",

"identified\_date": "2025-02-20",

"due\_date": "2025-03-06",

"mitigation\_plan": "Upgrade to TLS 1.3",

"status": "Completed",

"completion\_date": "2025-02-28"

}

]

}

**Value Addition:** **Enables agencies to track risk trends, monitor SLA adherence, and automate compliance checks.**

**7.2 Quarterly Vulnerability Scanning Report**

**Purpose:** Demonstrates CSP vulnerability management effectiveness.

**Structured Template**

{

"scan\_date": "2025-03-01",

"csp\_name": "SecureCloudGov",

"scanned\_systems": [

{

"system": "App Server Cluster",

"critical\_findings": 5,

"high\_findings": 12,

"medium\_findings": 30,

"remediation\_rate": "85%"

},

{

"system": "Database Cluster",

"critical\_findings": 2,

"high\_findings": 8,

"medium\_findings": 25,

"remediation\_rate": "90%"

}

]

}

**Value Addition:** **Automated API integration ensures agencies receive near-real-time vulnerability insights.**

**7.3 Annual Security Control Assessment Report**

**Purpose:** Validates adherence to FedRAMP controls.

**Structured Template**

{

"assessment\_period": "2025",

"csp\_name": "SecureCloudGov",

"controls": [

{

"control\_family": "Access Control",

"control\_id": "AC-2",

"control\_name": "Account Management",

"assessment\_result": "Pass",

"remediation\_plan": "N/A"

},

{

"control\_family": "System & Communications",

"control\_id": "SC-12",

"control\_name": "Cryptographic Key Management",

"assessment\_result": "Fail",

"remediation\_plan": "Migrate to FIPS 140-3 compliant HSM"

}

]

}

**Value Addition:** **Transforms compliance assessments into an actionable risk intelligence tool.**

**7.4 Incident Reporting Template (60-Minute Notification & 24-Hour Follow-Up)**

**Purpose:** Ensures immediate and detailed incident transparency.

**Structured Template**

{

"incident\_id": "INC-20250315-001",

"date\_detected": "2025-03-15T12:45:00Z",

"incident\_type": "Unauthorized Access",

"affected\_systems": ["GovCloud East – Database Cluster"],

"impact\_level": "High",

"initial\_mitigation\_action": "Account Lockdown, SIEM Investigation Initiated",

"follow\_up": {

"root\_cause\_analysis": "Compromised credentials due to phishing attack.",

"resolution\_steps": [

"MFA enforcement strengthened",

"Privileged access review conducted"

],

"lessons\_learned": "Additional employee phishing awareness training required."

}

}

**Value Addition:** **Automates threat intelligence sharing, accelerating agency response times.**

**7.5 API Schema for Automated Report Ingestion**

**Purpose:** Enables **seamless integration** of CSP reports with **agency SIEM, CDM, and FedRAMP dashboards**.

**API Endpoint: /api/v1/conmon-reports**

**Method:** POST  
**Content-Type:** application/json

**API Request Schema**

{

"report\_type": "poam",

"reporting\_period": "2025-03",

"csp\_name": "SecureCloudGov",

"data": {

"poam\_id": "POAM-001",

"vulnerability\_name": "OpenSSH Privilege Escalation",

"severity": "High",

"identified\_date": "2025-03-01",

"due\_date": "2025-03-15",

"mitigation\_plan": "Patch to OpenSSH v9.3",

"status": "In Progress",

"expected\_completion\_date": "2025-03-12"

}

}

**Value Addition:**

* **Automates report submissions**, eliminating manual uploads.
* **Enhances security intelligence sharing** for **real-time risk validation**.

**8. Compliance Checklists for FedRAMP Rev 5 and Rev 4 CSPs**

**8.1 FedRAMP Rev 5 Compliance Checklist**

**Authentication & Access Control**

* Multi-factor authentication (MFA) enabled for all privileged accounts.
* Just-in-time (JIT) privileged access implemented.

**Encryption & Data Protection**

* All data encrypted at rest using FIPS 140-3 validated cryptographic modules.
* TLS 1.3 enforced for all external connections.

**Threat Monitoring & Incident Response**

* SIEM solutions ingest logs from all critical systems.
* Incident response plan tested bi-annually.

**Value Addition:** Ensures CSPs align with the latest FedRAMP security expectations while reducing audit overhead.

**8.2 FedRAMP Rev 4 to Rev 5 Transition Checklist**

**Gap Analysis & Documentation**

* Conducted gap analysis of Rev 4 vs. Rev 5 controls.
* Submitted transition plan to FedRAMP PMO.

**Security Enhancements**

* Integrated Continuous Authorization to Operate (cATO) methodology.
* Automated vulnerability scanning and reporting workflows.

**Regulatory Compliance**

* Mapped security controls to NIST 800-53 Rev 5.
* Updated System Security Plan (SSP) with new control implementations.

**Value Addition:** Helps CSPs navigate a structured and transparent migration to FedRAMP Rev 5 while minimizing compliance risk.

**9. Key Value Additions of Enhanced ConMon Reporting**

This standard introduces **automation, standardization, and real-time risk intelligence** to **empower agencies with actionable insights**:

* **Proactive Risk Management** – Enables security teams to **validate CSP risk postures instantly**, reducing exposure to emerging threats.
* **Automated Compliance Audits** – Structured JSON/XML report formats ensure **seamless integration** with **SIEMs and CDM dashboards**.
* **Accelerated FedRAMP Rev 5 Adoption** – Provides CSPs on **Rev 4 a clear migration roadmap**, bridging compliance gaps efficiently.
* **Enhanced Regulatory Alignment** – Aligns with **NIST 800-53 Rev 5, Zero Trust Architecture (ZTA), and Continuous Diagnostics and Mitigation (CDM)** for seamless compliance.

**10. Conclusion**

By standardizing **structured reporting, automation, and API-driven integrations**, this framework **elevates ConMon from a compliance exercise to a real-time security intelligence capability**. **Agency security professionals gain instant visibility into CSP risk postures**, enabling **proactive and risk-based decision-making**.