POA&M Template Updates: Service Name Column and Configuration Findings Tab

On March 29, 2024, we posted updates to the FedRAMP Plan of Actions and Milestones (POA&M) Template located on the FedRAMP website.

Rev. 5 POA&M Service Name Column
We added the ‘Service Name’ column to the POA&M template for Agencies to understand which vulnerabilities apply to the CSO services, sub services and features that each Agency may be leveraging. This allows the POA&M user to filter the template to the items affecting their agency by the services or offerings purchased from the cloud service provider (CSP).

A	B	C	D	E	AE
FedRAMP® Plan of Action and Milestones (POA&M) Template					
CSP	**System Name**	**Impact Level**	**POAM Date**		
POAM ID	**Controls**	**Weakness Name**	**Weakness Description**	**Weakness Detector Source**	**Service Name**
Unique identifier for each POAM Item	Applicable 800-53 Control(s)	Name of the weakness as provided by the scanner or otherwise summarizing the weakness	Description of the weakness and other information	The scanner name or other source that detected the vulnerability	The associated service this vulnerability affects on the CSPs system. This should be the unique name (no shorthand) of the service/offering as the purchaser would see it Each service/offering should be separated by a new line (Alt+Enter)
Unique Identifier	Control Number	Text	Text	[Nessus, Qualys, Webinspect, Security Assessment Report, etc]	Text
V-1Example	*AC-1*	*Open port on Example Firewall*	*Unprovisioned port left open on example firewall*	*Nessus*	*Flux Capacitor* *Fire Bolt* *Clean Sweep* *Aeromancer*

Instructions For Use
This 'Service Name' cell (found in Column AE in the POA&M) should contain the name of each CSP's FedRAMP-authorized service(s) impacted by the vulnerability represented in each POA&M item row.

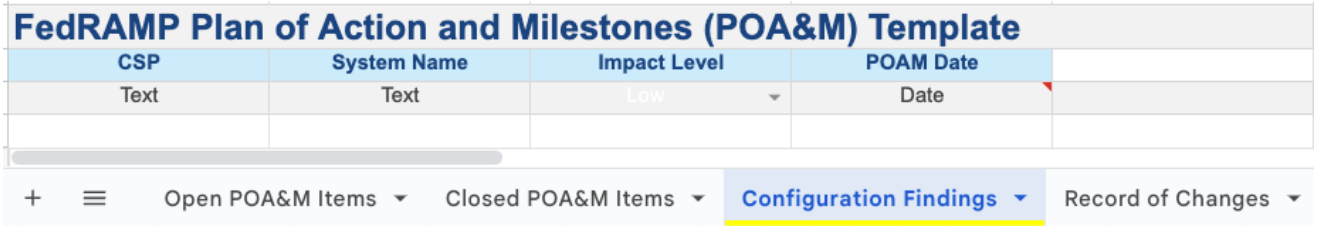
- Leave this cell blank if you do not offer individual services and features.
- This cell should capture the service(s) or feature(s) affected by the vulnerability represented in the same row of the POA&M document.
- This should be the unique name (e.g., no shorthand) of the service(s) or offering(s) known by the purchaser as represented by the FedRAMP Marketplace "Authoritative Source" and as advertised on the CSP's website.*
- Each service or offering should be separated by a new line within the cell (use: Alt+Enter).
- Mark as 'All' if the vulnerability affects the entire boundary.
- Mark as 'Internal' if the vulnerability only affects internal aspects of the boundary and no services.**

*We try to pre-address items that could confuse your agency customers.
**All leveraging entities should consider all 'Internal' findings when assessing risk postures.

Implementation Requirements
FedRAMP understands the implementation of this cell will require significant re-engineering by the CSP. FedRAMP requires this cell to be fully used by all CSPs by January 1, 2025. The Authorizing Official (AO) needs progress made and the schedule for status updates for the final implementation via an email no later than October 1, 2024.

Failure to meet the January 1, 2025 implementation date will result in the CSP adding a high POA&M item to track the status of this requirement. Per FedRAMP requirements, High POA&M items must be closed within 30 days of POA&M origination.

Rev. 5 POA&M Configuration Findings Tab
We added a 'Configuration Findings' tab. This will allow all Third Party Assessment Organizations (3PAO) to recognize these configuration deficiencies for easy validation.



Updates for FedRAMP CM-6 Deficiencies Recorded and Reported
FedRAMP requires compliance checks to evaluate configuration settings. CSPs and 3PAOs typically combine compliance check findings into a single CM-6 finding, which is acceptable. However, for initial assessments, annual assessments, and significant change requests, FedRAMP requires a clear understanding, on a ***per-control basis***, where risks exist. Therefore, 3PAOs must also analyze compliance check findings (e.g., compliance scans as part of the security controls assessment). If a direct mapping exists, the 3PAO must document additional findings ***per control*** in the corresponding Security Assessment Report (SAR) Risk Exposure Table (RET) and the CSP's POA&M. This will likely result in the details of individual control findings overlapping with those in the combined CM-6 finding.

During monthly continuous monitoring, new findings from CSP compliance checks may be combined into a single CM-6 POA&M item. CSPs are not required to map the findings to specific controls because controls are only assessed during initial assessments, annual assessments, and significant change requests.

NIST SP 800-53 Revision 5, CM-6 Configuration Settings, requires that all systems:

- Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using:
  - **DoD STIGS, or CIS Level 2** secure configurations for Moderate and High baseline systems, and
  - **DoD STIGS or CIS benchmarks** for Low and LI-SaaS baseline systems.
  - It is the service provider's responsibility to ensure the checklists for configuration settings are **Security Content Automation Protocol** (SCAP) validated or SCAP compatible (if validated checklists are not available).
- Implement the configuration settings.
- Identify, document, and approve any deviations from established configuration settings for all system components based on organization-defined operational requirements, and
- Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

LI-SaaS systems must also document and assess the CM-6 control to meet FedRAMP compliance; the least functionality details are required for that documentation.

Recording CM-6 Failures
3PAOs are required to define each configuration deficiency in the RET Workbook. Later, the CSP must record each CM-6 finding in the POA&M 'Configuration Findings' tab. As noted above, for initial assessments, annual assessments, and significant change requests, FedRAMP requires a clear understanding, on a ***per-control basis***, where risks exist. Therefore, 3PAOs must analyze and document compliance check findings as part of the controls assessment.

If you have any questions about these updates to the POA&M template , please email info@fedramp.gov.