



GOVRAMP CONTINUOUS MONITORING MATRIX TEMPLATE COMPLETION GUIDE OVERVIEW

VERSION:

1.0

DATE:

January 30, 2026



DOCUMENT REVISION HISTORY

Date	Description	Version	Author
1/30/2026	Initial Release	1.0	GovRAMP PMO
<Date>	<Revision Description>	<Version>	<Author>

HOW TO CONTACT US

For questions about GovRAMP, or for technical questions about this document including how to use it, contact pmo@GovRAMP.org. For more information about the GovRAMP program, see www.GovRAMP.org.



TABLE OF CONTENTS

1. ABOUT THIS DOCUMENT	1
2. WHO SHOULD USE THIS DOCUMENT?.....	1
3. POA&M PURPOSE.....	1
3.1 SCOPE	2
3.2 GENERAL REQUIREMENTS.....	2
4. CONTINUOUS MONITORING MATRIX TEMPLATE.....	4
4.1 TAB: EXECUTIVE SUMMARY	5
4.2 TAB: OPEN POA&M	6
4.3 TAB: CLOSED POA&M	11
4.4 TAB: VULNERABILITY DEVIATION REQUEST.....	11
4.5 TAB: INVENTORY WORKBOOK.....	16
4.6 TAB: STATS SUMMARY SHEET	19



1. ABOUT THIS DOCUMENT

This document provides guidance on completing the Government Risk and Authorization Management Program (GovRAMP) Continuous Monitoring Matrix template in support of achieving and maintaining a security authorization that meets GovRAMP requirements.

A Service Provider receiving a GovRAMP verified status (Core, Ready, Provisionally Authorized, or Authorized) must establish and maintain a Continuous Monitoring Matrix for their system in accordance with this Continuous Monitoring Matrix Completion Guide. The template is available at: www.govramp.org.

This guide aids in developing and overseeing Continuous Monitoring activities that align with GovRAMP standards. The Continuous Monitoring Matrix is required for security authorization and ongoing monitoring. It highlights any weaknesses in the system's security and outlines the steps the Service Provider will take to address them.

The template provides a structured format for organizing and updating Continuous Monitoring submissions. Service Providers are not permitted to alter or delete existing column headers, but additional information can be inserted to the far right of the set template.

2. WHO SHOULD USE THIS DOCUMENT?

This document is intended to be used by Service Providers, Government Agencies and other Public Sector entities, Third Party Assessment Organizations (3PAOs), or other advisory organizations.

3. POA&M PURPOSE

The purpose of the Plan of Action and Milestones (POA&M) is to facilitate a disciplined and structured approach to tracking risk mitigation activities in accordance with GovRAMP requirements. The POA&M includes security findings for the system from periodic security assessments and ongoing continuous monitoring activities. The POA&M includes the Service Provider's intended corrective actions and current disposition for those findings.

GovRAMP PMO uses the POA&M to monitor the Service Provider's progress in correcting these findings. The POA&M includes the:

- Security categorization of the cloud information system;
- Specific weaknesses or deficiencies in deployed security controls;



- Importance of the identified security control weaknesses or deficiencies;
- Scope of the weakness in components within the environment; and
- Proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security control implementations (e.g., prioritization of risk mitigation actions and allocation of risk mitigation resources).

The POA&M identifies:

- The tasks the Service Provider plans to accomplish, including a recommendation for completion either before or after information system implementation;
- Any milestones the Service Provider has set in place for meeting the tasks; and
- The scheduled completion dates the Service Provider has set for each milestone.

3.1 Scope

The scope of the POA&M includes security control implementations, including all management, operational, and technical implementations, that have unacceptable weaknesses or deficiencies. Once a Service Provider has obtained a Verified Status, they are required to submit an updated POA&M in the appropriate cadence for their GovRAMP Verified Status.

3.2 General Requirements

The Service Provider must include the following in the *Open POA&M Items* worksheet:

- All security vulnerabilities identified through vulnerability or policy compliance scanning tools at time of discovery.
- All known security vulnerabilities and deficiencies identified through means other than vulnerability scanning tools (e.g., interviews and penetration testing).
- All security vulnerabilities for which the Service Provider is submitting a Deviation Request.

A security vulnerability remediation is late if it is not remediated within the time requirements detailed in the *GovRAMP Continuous Monitoring Strategy & Improvement Guide* and summarized in the bullets below.

The Service Provider must comply with the following:

- Use the POA&M template found in the *GovRAMP Continuous Monitoring Matrix* to track and manage POA&M items.
- If a finding is identified in the Ready Assessment Report (RAR), Security Assessment Report (SAR), Risk Exposure Table (RET), or as a result of continuous monitoring activities, it must be included as an item on the POA&M.
- All POA&M entries must map back to a finding in the RAR, SAR, and/or continuous monitoring activities.



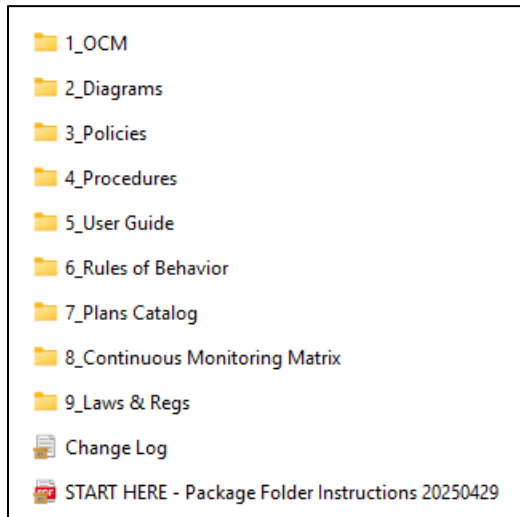
- False positives identified in the RAR or SAR, along with supporting evidence (e.g., clean scan report) do not have to be included in the POA&M.
- Each finding in the POA&M must have a unique identifier. This unique identifier must pair with a respective RAR or SAR finding and continuous monitoring activities.
- Critical risk findings identified through continuous monitoring activities should be remediated as soon as possible and must be remediated within 30 days after identification.
- High, Moderate, and Low risk findings must be remediated within the timeline specified in RA-05.



4. CONTINUOUS MONITORING MATRIX TEMPLATE

The *GovRAMP Continuous Monitoring Matrix_Rev 5* template can be found within the Service Providers Package Low/Moderate Impact (8_Continuous Monitoring Matrix folder). Refer to the document library on the GovRAMP website.

Image 1: Impact Service Providers Package



The *GovRAMP Continuous Monitoring Matrix_Rev 5* template contains the following tabs:

- *Executive Summary*
- *Open POA&M*
- *Closed POA&M*
- *Vulnerability Deviation Request*
- *Inventory Workbook*
- *Stats Summary Sheet*



4.1 TAB: Executive Summary

Term definitions/explanations for the tab:

SECTION	ROW/COLUMN	DETAILS
System Information	Service Provider Name	The Service Provider name as supplied in the documents provided to GovRAMP.
	Information System Name	The information system name as supplied in the documents provided to GovRAMP.
	Version	System version.
	Date	The date the POA&M was last updated.
	Impact Level	Cloud Service Offerings (CSOs) are categorized as <i>Low</i> , <i>Moderate</i> , or <i>High</i> based on the <i>GovRAMP Data Classification Tool</i> document.
	GovRAMP Package ID	This is a unique GovRAMP number identifying each package. This can be obtained from your Membership Engagement Team representative.
Open POA&M Summary	High	This number is based on original risk rating of <i>High</i> .
	High -> Moderate (RA)	This number is based on an original risk rating of <i>High</i> that has received a risk adjustment to <i>Moderate</i> .
	Moderate	This number is based on original risk rating of <i>Moderate</i> .
	Moderate -> Low (RA)	This number is based on an original risk rating of <i>Moderate</i> that has received a risk adjustment to <i>Low</i> .
	Low	This number is based on original risk rating of <i>Low</i> .
	Total <i>Auto-calculates, no provider input needed</i>	The sum of all open <i>High</i> vulnerabilities, <i>Moderate</i> vulnerabilities, and <i>Low</i> vulnerabilities.
POA&M Aging	0-30	The sum of each risk level that has aged 0-30 days from original detection date. <i>These are not considered past due.</i>
	31-90	The sum of each risk level that has aged 31-90 days from original detection date. <i>These are not considered past due for Moderate and Lows.</i>
	91-180	The sum of each risk level that has aged 91-180 days from original detection date. <i>These are not considered past due for Lows.</i>



SECTION	ROW/COLUMN	DETAILS
	181+	The sum of each risk level that has aged greater than 181 days from original detection date.
	Total Past Due	This horizontal sum by risk level for 31 or more days past discovery. This cell automatically calculates.
	Total	This vertical cell is the sum of each aging column that is past due: 31-90, 91-180, 181+ days.
Deviations	New False Positive/Operational Requirement/Risk Adjustment	Total number of new False Positive (FP), Operational Requirement (OR), and/or Risk Adjustment (RA) for the reporting month.
	Pending/Active False Positive/Operational Requirement/Risk Adjustment	Sum of all Pending or Active (Yes) False Positives (FP), Operational Requirements (OR), and/or Risk Adjustments (RA) from the <i>Open POA&M</i> tab.
Scan Files Submitted	<p>Please refer to the listed file naming standards for uploaded files.</p> <p>Add a suffix if you have multiple files in the same category.</p>	<p>File Naming Standards:</p> <p>OS Scans: mm_yyyy_OS_yourfilename</p> <p>DB Scans: mm_yyyy_DB_yourfilename</p> <p>Web Scans: mm_yyyy_web_yourfilename</p> <p>Container Scans: mm_yyyy_container_yourfilename</p> <p>Compliance (DISA STIGs) Scans: mm_yyyy_compliance_yourfilename</p>
Comment or Items to Note		Service Providers can provide additional information pertaining to the current month's submission.

4.2 TAB: Open POA&M

The *Open POA&M* tab includes the corrective action plan used to track security weaknesses. This worksheet has similarities to the National Institute of Standards and Technology's (NIST) format requirements; however, it contains additional data and formatting as required by GovRAMP.

NOTE: Do not insert any columns between the columns listed below.

Term definitions/explanations for the tab:



COLUMN	DETAILS
POA&M ID	<p>Assign a unique identifier to each POA&M item. This identifier is assigned by the Service Provider to a unique vulnerability in the Service Provider's system. Often, during annual assessment activities the 3PAO identifies a vulnerability that the Service Provider has already identified through continuous monitoring activities, or vice versa. If the same vulnerability is detected on the same assets, the same POA&M ID must be used by both parties. The earlier of the two detection dates applies. If the same vulnerability is discovered on additional assets at a later date, a new POA&M ID and detection date may be used for the new assets.</p> <p>Suggested naming conventions: V for vulnerability, W for web application, P for policy compliance (e.g., P-123).</p>
Controls	<p>Specify the GovRAMP security Control ID affected by the weakness identified during the security assessment process.</p>
Weakness Name	<p>Specify a name for the identified weakness that provides a general idea of the weakness. Use the weakness name provided by the security assessor or taken from the vulnerability scanner that discovered the weakness.</p>
Weakness Description	<p>Describe the weakness identified during the assessment process. Use the weakness description provided by the security assessor or the vulnerability scanner that discovered the weakness. Provide sufficient data to facilitate oversight and tracking. This description must demonstrate awareness of the weakness and facilitate the creation of specific milestones to address the weakness. In cases where it is necessary to provide sensitive information to describe the weakness, italicize the sensitive information to identify it and include a note in the description stating that it is sensitive.</p>
Weakness Detector Source	<p>Specify the name of the 3PAO, vulnerability scanner, or other entity that first identified the weakness. In cases where there are multiple 3PAOs, include each one on a new line.</p>
Weakness Source Identifier	<p>Often, the scanner/assessor will provide an identifier (ID/Reference #) that specifies the weakness in question. This allows further research into the weakness. Provide the identifier, or state that no identifier exists.</p> <p>If the Service Provider identifies the same weakness source identifier across multiple assets, consolidate the weakness into a single finding and report all the affected assets in Column G (<i>Asset Identifier</i>).</p>
Asset Identifier	<p>List the asset/platform on which the weakness was found. This must correspond to the <i>Unique Asset Identifier</i> for the item provided in the <i>Inventory Workbook</i> tab. Include a complete asset identifier for each affected asset. Do not use an abbreviation or "shorthand." The asset identifier must be unique and consistent across all POA&M documents, 3PAOs, and any vulnerability scanning tools.</p>
Point of Contact	<p>Identify the person/role that the Service Provider holds responsible for resolving each reported weakness.</p>
Resources Required	<p>Identify resources required for resolving the weakness.</p>



COLUMN	DETAILS
Overall Remediation Plan	Provide a high-level summary of the actions required to remediate the weakness. In cases where it is necessary to provide sensitive information to describe the remediation plan, italicize the sensitive information to identify it and include a note in the description stating that it is sensitive. Often, the scanner/assessor will provide a remediation plan for the weakness in question.
Original Detection Date	<p>Provide the month, day, and year when the weakness was first detected. This must be consistent with the Security Assessment Report (SAR) and/or the scan dates identified from the continuous monitoring activities. The Service Provider may not change the original detection date.</p> <p>If a previously remediated vulnerability is detected, use the date from the first time the vulnerability was detected. Additionally, make sure to update Column Z (<i>Comments</i>) to include the note "Reoccurring" along with the date when it was detected again.</p>
Scheduled Completion Date	<p>A scheduled completion date is required for every weakness. It must include month, day, and year.</p> <p>The scheduled completion date will be based on the original risk rating of the weakness and the required remediation timeframes specified in RA-5.</p> <p>If the weakness has an adjusted risk rating and states "Pending" or "Yes" in Column U (<i>Risk Adjustment</i>), the adjusted risk rating will take precedence over the original risk rating.</p> <p>The scheduled completion date must not change once it is recorded, unless approved by the PMO as a risk adjustment.</p>
Planned Milestones	Every weakness must include milestones that outline how the vulnerability will be addressed along with estimated milestone completion dates. This should include any incremental progress planned towards full remediation.
Milestone Changes	Provide any updates or modifications to the previously planned milestones. These updates should include any incremental progress made towards full remediation.
Status Date	Provide the latest date an action was taken to remediate the weakness, or some change was made to the POA&M item. Each POA&M item should have a status date within 30 days prior to the date listed on the <i>Executive Summary</i> tab.



COLUMN	DETAILS
Vendor Dependency	<p>This indicates the remediation of the weakness required by the action of a third-party vendor (e.g., through the issuing of a patch that is not yet released). The Service Provider is required to check the status of the vendor's fix for the vulnerability at least once every 30 days.</p> <p>If the fix is still pending from the vendor, and the Service Provider has checked in with the vendor within 30 days of POA&M submission, GovRAMP will not count the entry as late.</p> <p>Once the vendor makes the fix available, the Service Provider has the timeframes specified in RA-5 to remediate the vulnerability. The Service Provider must provide the vendor's release date in Column Z (<i>Comments</i>). In this case, the Service Provider may overwrite the auto-calculated scheduled completion date found in Column L (<i>Scheduled Completion Date</i>).</p> <p>If a vendor dependency is ongoing, a Service Provider may have to migrate to a different technology/vendor.</p>
Last Vendor Check-in Date	<p>This column is used to record the date the Service Provider most recently checked in with a third-party vendor regarding the availability of an un-released remedy for a known product vulnerability. If <i>Vendor Dependency</i> is "Yes," the Service Provider must check-in with the third-party vendor at least once every 30 days and record the most recent date of check-in here. If <i>Vendor Dependency</i> is "No," the Service Provider should leave this column blank.</p>
Vendor Dependent Product Name	<p>If <i>Vendor Dependency</i> is "Yes," the Service Provider must provide the name of the product of which the third-party vendor has responsibility. If <i>Vendor Dependency</i> is "No," the Service Provider should leave this column blank.</p>
Original Risk Rating	<p>Provide the original risk rating of the weakness at the time it was identified as part of an assessment and/or continuous monitoring activities.</p>
Adjusted Risk Rating	<p>Enter the adjusted risk rating after a risk adjustment for the vulnerability is created on the <i>Vulnerability Deviation Request</i> tab.</p> <p>If no risk adjustment is made, enter "N/A" or leave this cell blank.</p> <p>In the case that the scanner changes its risk rating from a lower to a higher risk rating, the Service Provider must update this column and set <i>Risk Adjustment</i> to "Yes". No deviation request form is necessary in this case.</p>
Risk Adjustment	<p>If the Service Provider believes a risk adjustment is appropriate, they must set this column to "Pending" and create an entry in the <i>Vulnerability Deviation Request</i> tab. When creating a deviation request, follow the guidance in Section 4.4 <i>Tab: Vulnerability Deviation Request</i> and complete the GovRAMP <i>Deviation Request Supporting Documentation</i> form.</p> <p>If the PMO approves the deviation request, the Service Provider must change this entry to "Yes". If the PMO denies the deviation request, or if the Service Provider does not intend to request a risk adjustment, the Service Provider must set this entry to "No".</p> <p>Only PMO-approved risk adjustments may alter the scheduled completion date.</p>



COLUMN	DETAILS
False Positive	<p>A false positive (FP) occurs when a vulnerability is identified that does not actually exist on the system. This is known to happen from time to time with scanning tools.</p> <p>If the Service Provider believes a finding is an FP, they must set this column to "Pending" and create an entry in the <i>Vulnerability Deviation Request</i> tab. When creating a deviation request, follow the guidance in Section 4.4 <i>Tab: Vulnerability Deviation Request</i> and complete the <i>GovRAMP Deviation Request Supporting Documentation</i> form.</p> <p>If the PMO approves the deviation request, the Service Provider must change this entry to "Yes". If the PMO denies the deviation request, or if the Service Provider does not believe the finding is an FP, the Service Provider must set this entry to "No".</p> <p>PMO-approved false positives can also be closed; see Section 4.3 <i>Tab: Closed POA&M</i> for guidance on closing a POA&M item.</p>
Operational Requirement	<p>An operational requirement (OR) indicates that there is an open vulnerability in the system that cannot be addressed without affecting the system's overall functionality or contradicting contractual requirements. An OR can be exploited regardless of the limited opportunity for exploitation, such as a component that is installed but not enabled.</p> <p>If the Service Provider believes a finding is an OR, they must set this column to "Pending" and create an entry in the <i>Vulnerability Deviation Request</i> tab. When creating a deviation request, follow the guidance in Section 4.4 <i>Tab: Vulnerability Deviation Request</i> and complete the <i>GovRAMP Deviation Request Supporting Documentation</i> form.</p> <p>If the PMO approves the deviation request, the Service Provider must change this entry to "Yes". If the PMO denies the deviation request, or if the Service Provider does not believe the finding is an OR, the Service Provider must set this entry to "No".</p> <p>Approved ORs must remain on the <i>Open POA&M</i> tab, be periodically reassessed by the Service Provider, and assessed annually by a Third-Party Assessor Organization (3PAO).</p>
Deviation Rationale	<p>Provide a rationale for any deviation request submitted to the PMO. For operational requirements and risk adjustments, include mitigating factors and compensating controls that address the specific risk to the system. For false positives, include information about evidence/artifacts that support the result. This information is to be included in the <i>GovRAMP Deviation Request Support Documentation</i>.</p>
Supporting Documents	<p>List any additional documents that are associated with the POA&M item. This must include a <i>Deviation Request Supporting Documentation</i> form.</p>
Comments	<p>Provide any additional comments that have not been provided in any of the other columns.</p> <p>For vendor dependencies, the Service Provider must provide the vendor's release date (this is the date the vendor makes the fix available).</p> <p>For reoccurring vulnerabilities that were previously closed, make sure to include the note "Reoccurring" along with the date when it was detected again.</p>



4.3 TAB: Closed POA&M

The *Closed POA&M* tab contains the same system information columns as the top of the *Open POA&M* tab. The remainder of the tab contains the POA&M items that are completed. The details should reflect all the information provided in the *Open POA&M* tab.

A POA&M item can be moved to the *Closed POA&M* tab when either of the following occurs:

- The Service Provider has implemented all necessary corrective actions and gathered evidence of mitigation, which will be stored for future inspections. This evidence could be reviewed by a 3PAO during both initial and regular assessments and may also be requested by the GovRAMP PMO at any point.
- A false positive deviation request has been approved by the GovRAMP PMO.

To “close” a POA&M item:

- Move the POA&M item to the *Closed POA&M* tab.
- Update the date in Column O (*Status Date*) with the “closed” date.
- Update the date in Column N (*Milestone Changes*) and specify how the vulnerability was fixed and how the fix was verified.

4.4 TAB: Vulnerability Deviation Request

When the Service Provider identifies a vulnerability that potentially warrants different handling than normally required by GovRAMP, the Service Provider will need to submit a deviation request to GovRAMP in the *Vulnerability Deviation Request* tab of the *GovRAMP Continuous Monitoring Matrix*.

All deviation requests should reflect a pending status in the *Open POA&M* tab of the *GovRAMP Continuous Monitoring Matrix* until reviewed and adjudicated by:

- The 3PAO during your annual or initial assessment; or
- The GovRAMP PMO outside of the annual or initial assessment

Deviation request types include:

- False Positive (FP): A finding that incorrectly indicates a vulnerability is present, where none exists. Justified through documentation and evidence.
- Risk Adjustment (RA): A reduction in the scanner-cited risk level of a finding. Accomplished through existing or new compensating controls that reduce likelihood and/or impact of exploitation.
- Operational Requirement (OR): A finding that cannot be remediated, often because the system will not function as intended, or because a vendor explicitly indicated it does not intend to offer a fix to their product. Service Providers will need to document the



compensating controls in place and seek ways to mitigate the risk associated with ORs. GovRAMP will not approve an OR for a High vulnerability; however, the service provider may mitigate the risk.

- An operational requirement cannot be marked as a false positive.
- RA & OR: A single deviation request may simultaneously justify a risk adjustment and an operational requirement.

NOTE: A Vendor Dependency does not require a deviation request.

Term definitions/explanations for the tab:

COLUMN	SUBCOLUMN	DETAILS
DR Number		Each deviation request should have their own <i>DR Number</i> . The <i>DR Number</i> increases in increments of 1 for each subsequent deviation request and should not be reused.
Vulnerability Information	POA&M ID	A unique identifier that was assigned to the POA&M on the <i>Open POA&M</i> tab.
	Scan ID	Often, the scanner/assessor will provide an identifier (ID/Reference #) that specifies the weakness in question. This allows further research of the weakness. Provide the identifier, or state that no identifier exists.
	Assets Impacted	List the asset/platform on which the weakness was found. This must correspond to the <i>Asset Identifier</i> for the item provided in the <i>Inventory Workbook</i> tab and <i>Open POA&M</i> tab.
	Vulnerability Name	Provide the name of the vulnerability. This should be the <i>Weakness Name</i> listed on the <i>Open POA&M</i> tab.
	Vulnerability Source	Specify the name of the 3PAO, vulnerability scanner, or other entity that first identified the weakness. In cases where there are multiple 3PAOs, include each one on a new line.
	Initial Risk Rating	Provide the original risk rating of the weakness at the time it was identified as part of an assessment and/or continuous monitoring activities.
	Original Detection Date	Provide the month, day, and year when the weakness was first detected. This must be consistent with the Security Assessment Report (SAR) and/or the scan dates identified from the continuous monitoring activities.



COLUMN	SUBCOLUMN	DETAILS
	Tool-Provided Vulnerability Description	Describe the weakness identified during the assessment process. Use the <i>Weakness Description</i> provided by the security assessor or the vulnerability scanner that discovered the weakness. Provide sufficient data to facilitate oversight and tracking. This description must demonstrate awareness of the weakness and facilitate the creation of specific milestones to address the weakness. In cases where it is necessary to provide sensitive information to describe the weakness, italicize the sensitive information to identify it and include a note in the description stating that it is sensitive.
	Tool-Provided Recommended Action	Describe the recommended action(s) to remediate the identified vulnerability. Use the recommended action provided by the security assessor or the vulnerability scanner that discovered the weakness.
	SP-Provided Vulnerability Information (Optional)	Provide any additional information regarding the vulnerability here. This cell is optional.
Deviation Request Summary	Type of DR	List the type of deviation you are requesting (i.e. false positive, operational requirement, risk adjustment).
	Requested Risk Rating/Impact	If requesting an RA or an OR with an RA, please provide the adjusted risk you are requesting in this cell. NOTE: You may only risk adjust up or down one level.
	DR Submission Date	Date you are submitting this deviation request.
	DR Rationale	Detail justification for your deviation request.
Additional Information: False Positive	Evidence Description	Detail the evidence you submitted for a false positive. You may utilize the <i>Deviation Request Supporting Documentation</i> form to provide additional details.
	List of Evidence Attachments	List of file name(s) of evidence submitted for this deviation, such as screenshots.
Additional Information: Operational Requirement	Operational Impact Statement	Detail the limitations that prevent the vulnerability from being fixed. Include negative operational impacts of remediation.
	Justification	For operational requirements, you must include an explanation of the limitations that prevent the finding from being fixed.
	List of Evidence Attachments	Provide authoritative links and screen shots of websites if this is for a 3rd party application or middleware. (SQL, SCCM, etc.)
Additional Information: Risk Adjustment	Attack Vector	Select whether local access, physical access, or network access is required for vulnerability exploitation.
	Attack Vector Explanation	Describe how, based on the SP's implemented security model, the necessary access is reduced or not available.



COLUMN	SUBCOLUMN	DETAILS
	Attack Complexity	<p><i>Low</i> attack complexity means that an attacker can exploit the vulnerability at any time and at all times.</p> <p><i>High</i> attack complexity means that a successful attack depends on conditions outside of the attacker's control.</p>
	Attack Complexity Explanation	<p>Describe the conditions beyond the attacker's control that must exist in order to exploit the vulnerability. Such conditions may require the collection of more information about the target, or computational exceptions.</p> <p>IMPORTANT: Exclude any requirements for user interaction in order to exploit the vulnerability (such conditions are captured in the <i>User Interaction</i> fields).</p>
	Privileges Required	<p>Select the level of privileges an attacker must possess before successfully exploiting the vulnerability.</p> <p><i>None</i> requires no privileges and can be exploited by an unauthorized user.</p> <p><i>Low</i> privileges require a normal authenticated user to exploit the vulnerability.</p> <p><i>High</i> privileges require an Administrator or System level authenticated user to exploit the vulnerability.</p>
	Privileges Required Explanation	<p>Describe any security controls that prevent or reduce the likelihood of a vulnerability exploitation attempt having the required privileges on the system.</p>
	User Interaction	<p>Select whether the vulnerability can be exploited solely at the will of the attacker, or whether a separate user (or user-initiated process) must participate in some manner.</p> <p><i>None</i> means the vulnerable system can be exploited without interaction from a user.</p> <p><i>Required</i> means successful exploitation of this vulnerability requires a user to take some action before the vulnerability can be exploited.</p>
	User Interaction Explanation	<p>Describe any security controls that prevent or reduce the likelihood of necessary user interaction on the system.</p>
	Impact Metrics: Confidentiality	<p><i>High</i> if all information is disclosed to an attacker or some critical information is disclosed.</p> <p><i>Low</i> if some information can be obtained and/or the attacker does not have control over the kind or degree.</p> <p><i>None</i> if no information is disclosed.</p>



COLUMN	SUBCOLUMN	DETAILS
	Impact Metrics: Confidentiality Explanation	Measures the impact to the confidentiality of the information resources managed by a software component due to a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized ones.
	Impact Metrics: Integrity	<i>High</i> if an attacker can modify information at any time or only some critical information can be modified. <i>Low</i> if some information can be modified and the attacker does not have control over the kind or degree. <i>None</i> if there is no integrity loss.
	Impact Metrics: Integrity Explanation	Measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.
	Impact Metrics: Availability	<i>High</i> if an attacker can cause a resource to become completely unavailable or if the resource is a critical component and can become partially available. <i>Low</i> if an attacker can cause reduced performance or interrupt resources availability or response. <i>None</i> if there is no availability impact.
	Impact Metrics: Availability Explanation	Measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability. Attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of an impacted component.
	Remediation Level	Select from the drop-down whether the remediation is Official Fix, Temporary Fix, Workaround, or Unavailable.
	Remediation Level Explanation	<i>Official Fix</i> means that a complete vendor solution is available; either the vendor has issued an official patch or an upgrade is available. <i>Temporary Fix</i> means that there is an official but temporary fix available. This includes instances where the vendor issues a temporary hotfix, tool, or workaround. <i>Workaround</i> means that there is an unofficial, non-vendor solution available. In some cases, users of the affected technology will create a patch of their own or provide steps to work around or otherwise mitigate the vulnerability. <i>Unavailable</i> means that there is either no solution available or it is impossible to apply. Describe any remediation that has been taken to address the vulnerability on the affected system(s).
	List of Risk Reduction Attachments	Attach evidence, such as screen shots. List evidence attachments here.



COLUMN	SUBCOLUMN	DETAILS
Additional Information		Use this space to provide any additional information you believe is relevant to the deviation request.

4.5 TAB: Inventory Workbook

The Service Provider must continuously maintain an inventory workbook using the *Inventory Workbook* tab in the *GovRAMP Continuous Monitoring Matrix*. In accordance with the *GovRAMP Continuous Monitoring Guide*, the Service Provider must submit their up-to-date inventory workbook with their POA&M and other continuous monitoring deliverables.

The *Inventory Workbook* tab needs to contain ALL hardware components, software components, IaaS components, and PaaS services comprised in the entire information system. Not every column will be filled out for every row, and "N/A" can be used if the cell will not be populated.

Term definitions/explanations for the tab:

COLUMN	SUBCOLUMN	DETAILS
All Inventories	Unique Asset Identifier	<p>Unique identifier associated with the asset used consistently across all Service Provider documentation. This must correspond to the <i>Asset Identifier</i> for the item provided in the <i>Open POA&M</i> tab. For OS/Infrastructure and Web Application Software, this is typically an IP address or URL/DNS name as the component is identified by the scans. For a database, it is typically an IP address, URL, or database name. For containers, it is the repository/image name/version number.</p> <p>Mandatory and must be unique for all inventory records.</p>
	IPv4 and/or IPv6 Addresses	<p>If available, state the IPv4 and/or IPv6 addresses of the inventory item. This can be left blank if one does not exist, or if it is a dynamic field. If the IP address is used as the <i>Unique Asset Identifier</i>, then this field will duplicate the contents of the <i>Unique Asset Identifier</i> column.</p> <p>If a device has multiple IP addresses, then include one row in this inventory for each IP address. For containers, each entry should contain the individual checksum of the container in the registry for each of the containers in production that align to that image name/version.</p> <p>Mandatory for all inventory records.</p>



COLUMN	SUBCOLUMN	DETAILS
	Virtual	<p>Is this asset virtual?</p> <p>Mandatory for OS/Infrastructure, Containers, Software, and Databases.</p>
	Public	<p>Is this asset a public facing device? That is, is it outside the boundary? If so, it is an entry point.</p> <p>Mandatory for OS/Infrastructure, Containers, Software, and Databases.</p>
	DNS Name or URL	<p>If available, state the DNS name or URL of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.</p> <p>Optional, unless used as the identifier in vulnerability scans or security assessments.</p>
OS/Infrastructure Inventory	NetBIOS Name	<p>If available, state the NetBIOS name of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.</p> <p>Optional, unless used as the identifier in vulnerability scans or security assessments.</p>
	MAC Address	<p>If available, state the MAC Address of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.</p> <p>Optional, unless used as the identifier in vulnerability scans or security assessments.</p>
	Authenticated Scan	<p>Is the asset planned for an authenticated scan?</p> <p>Mandatory for OS/Infrastructure and Containers.</p>
	Baseline Configuration Name	<p>Name of the applicable Security Technical Implementation Guide(s) (STIGs), Center for Internet Security (CIS) Level 2 Benchmark(s), or relevant hardening benchmark(s).</p> <p>Mandatory for OS/Infrastructure and Containers.</p>
	OS Name and Version	<p>Operating system name and version running on the asset.</p> <p>Mandatory for OS/Infrastructure and Containers. Leave blank for Software and Database.</p>



COLUMN	SUBCOLUMN	DETAILS
	Location	Physical location of hardware. Could include Data Center ID, Cage #, Rack #, or other meaningful location identifiers. Optional for OS/Infrastructure. Leave blank for Containers, Software and Database.
	Asset Type	Simple description of the asset's function (e.g., Router, Storage Array, DNS Server, etc.) Mandatory for OS/Infrastructure and Containers. Leave blank for Software and Database.
	Hardware Make/Model	Name of the hardware product and model. Mandatory for OS/Infrastructure and Containers. Leave blank for Software and Database.
	In Latest Scan	Should the asset appear in the network scans, and can it be probed by the scans creating the current POA&M? Mandatory for OS/Infrastructure and Containers. Leave blank for Software and Database.
Software and Database Inventories	Software/Database Vendor	Name of container, software or database vendor. Mandatory for Software and Databases. Leave blank for OS/Infrastructure.
	Software/Database Name and Version	Name of software or database product and version number. Mandatory for Software and Databases. Leave blank for OS/Infrastructure.
	Patch Level	Patch version number. Optional if applicable.
	Function	The function provided by the component for the system. Mandatory for all assets/components.
Any Inventory	Comments	Any additional information that could be useful to the reviewer. Optional for OS/Infrastructure, Containers, Software and Databases.



COLUMN	SUBCOLUMN	DETAILS
	Serial Number/Asset Tag Number	Product serial number or internal asset tag #. Optional for OS/Infrastructure. Leave blank for Containers, Software and Database.
	VLAN/Network ID	Virtual LAN or network ID. Optional for OS/Infrastructure. Leave blank for Containers, Software and Database.
	System Administrator/Owner	Name of the system administrator or owner. Mandatory for all assets/components.
	Application Administrator/Owner	Name of the application administrator or owner. Optional for OS/Infrastructure. Leave blank for Containers, Software and Database.

4.6 TAB: Stats Summary Sheet

The *Stats Summary Sheet* tab serves as a tool that automatically compiles data from the *Open POA&M* tab, providing a comprehensive overview. This tab not only counts the total number of open POA&M entries, but also categorizes the vulnerabilities based on their severity levels—high, moderate, and low—specifically focusing on those that are past their due dates.

NOTE: This tab is designed for automatic updates and calculations; therefore, it should not be modified or altered to ensure the integrity of the data presented.

Term definitions/explanations for the tab:

ROW	DETAILS
POA&M Date	POA&M reporting date.
Open POAMs	Total number of open vulnerabilities.
Total Highs	Total number of open <i>High</i> risk vulnerabilities. This includes <i>Moderate</i> risk vulnerabilities that are risk adjusted to <i>High</i> risk.
Total Moderates	Total number of <i>Moderate</i> risk vulnerabilities. This includes <i>High</i> risk or <i>Low</i> risk vulnerabilities that are risk adjusted to <i>Moderate</i> risk.
Total Lows	Total number of <i>Low</i> risk vulnerabilities. This includes <i>Moderate</i> risk vulnerabilities that are risk adjusted to <i>Low</i> risk.



ROW	DETAILS
Vendor Dependencies – VD (Yes/Pending)	<p>Total number of vulnerabilities that are vendor dependencies.</p> <p>Vendor dependencies are vulnerabilities in which the remediation of the weakness is required by the action of a third-party vendor (e.g., through the issuing of a patch that is not yet released).</p> <p>The Service Provider is required to check the status of the vendor's remedy at least every 30 days. If this fix is still pending from the vendor, and the Service Provider has checked in with the vendor within 30 days of POA&M submission, GovRAMP will not count the entry as late.</p> <p>Once the vendor makes the fix available, the Service Provider must remediate the vulnerability within the appropriate timeframe for the assigned risk rating.</p>
Operational Requirements – OR (Yes/Pending)	<p>Total number of vulnerabilities that are operational requirements.</p> <p>Operational requirements are vulnerabilities present in a system that must remain open as correcting the vulnerability will impact the full operation of the system. Operational requirements may also be open vulnerabilities that can be exploited regardless of the limited opportunity for exploitation, such as a component that is installed but not enabled.</p> <p>Approved operational requirements must remain on the <i>Open POA&M</i> tab and be periodically reassessed by the Service Provider.</p>
False Positives – FP (Yes/Pending)	<p>Total number of vulnerabilities that are false positives.</p> <p>False positives are vulnerabilities, usually identified by scanning tools, that do not actually exist within the system.</p>
Total number of all Risk Adjustments	<p>Total number of vulnerabilities with risk adjustments. This includes risk adjustments that are pending review by GovRAMP PMO and risk adjustments that have been approved by GovRAMP PMO.</p> <p>Approved false positives should be moved to the <i>Closed POA&M</i> tab.</p>
Overdue Critical Vulnerabilities (Aged > 30 days) <i>Aged 31+ days</i>	<p>Total number of <i>Critical</i> risk vulnerabilities aged greater than 30 days.</p> <p>This does not include vulnerabilities marked as vendor dependencies, false positives, or operational requirements.</p> <p>If the Service Provider's POA&M reports one (1) or more <i>Critical</i> risk vulnerabilities are aged greater than 30 days, a GovRAMP deficiency trigger will be activated and GovRAMP PMO will send a notification to the Service Provider.</p>
Overdue High Vulnerabilities (Aged > 30 days) <i>Aged 31 – 60 days</i>	<p>Total number of <i>High</i> risk vulnerabilities aged greater than 30 days.</p> <p>This does not include vulnerabilities marked as vendor dependencies, false positives, or operational requirements.</p> <p>If the Service Provider's POA&M reports five (5) or more <i>High</i> risk vulnerabilities are aged greater than 30 days, a GovRAMP deficiency trigger will be activated and GovRAMP PMO will send a notification to the Service Provider.</p>



ROW	DETAILS
Overdue High Vulnerabilities (Aged > 60 days) <i>Aged 61+ days</i>	Total number of <i>High</i> risk vulnerabilities aged greater than 60 days. This does not include vulnerabilities marked as vendor dependencies, false positives, or operational requirements. If the Service Provider's POA&M reports five (5) or more <i>High</i> risk vulnerabilities are aged greater than 60 days, a GovRAMP deficiency trigger will be activated and GovRAMP PMO will send a notification to the Service Provider.
Overdue Moderate Vulnerabilities (Aged > 90 days) <i>Aged 91 – 180 days</i>	Total number of <i>Moderate</i> risk vulnerabilities aged greater than 90 days. This does not include vulnerabilities marked as vendor dependencies, false positives, or operational requirements. If the Service Provider's POA&M reports 10 or more <i>Moderate</i> risk vulnerabilities are aged greater than 90 days, a GovRAMP deficiency trigger will be activated and GovRAMP PMO will send a notification to the Service Provider.
Overdue Moderate Vulnerabilities (Aged > 180 days) <i>Aged 181+ days</i>	Total number of <i>Moderate</i> risk vulnerabilities aged greater than 180 days. This does not include vulnerabilities marked as vendor dependencies, false positives, or operational requirements. If the Service Provider's POA&M reports 10 or more <i>Moderate</i> risk vulnerabilities are aged greater than 180 days, a GovRAMP deficiency trigger will be activated and GovRAMP PMO will send a notification to the Service Provider.
Overdue Low Vulnerabilities (Aged > 180 days) <i>Aged 181+ days</i>	Total number of <i>Low</i> risk vulnerabilities aged greater than 180 days. This does not include vulnerabilities marked as vendor dependencies, false positives, or operational requirements.