Office of Audits
Office of Inspector General
U.S. General Services Administration

Audit of the Federal Risk and Authorization Management Program, Program Management Office's Goals and Objectives

Report Number A170023/Q/T/P19002
March 21, 2019

Executive Summary

Audit of the Federal Risk and Authorization Management Program, Program Management Office's Goals and Objectives
Report Number A170023/Q/T/P19002
March 21, 2019

Why We Performed This Audit

This audit was included in the GSA Office of Inspector General *Fiscal Year 2017 Audit Plan*. The initial focus for this audit was to review GSA's Federal Risk and Authorization Management Program (FedRAMP), Program Management Office's (PMO) authorization and accreditation process for third party providers. However, during our survey work, we determined that risks are present at the FedRAMP PMO level; therefore, we evaluated the FedRAMP PMO's goals and objectives to determine if they are sufficient to assess its effectiveness in accomplishing its mission.

What We Found

The FedRAMP PMO has not established an adequate structure comprising its mission, goals, and objectives for assisting the federal government with the adoption of secure cloud services. Specifically, the mission statement does not provide a clear direction for the FedRAMP PMO; objective statements are missing key attributes; and the alignment of the mission, goals, and objective statements makes it difficult to determine if the FedRAMP PMO is meeting its mission in an effective manner.

What We Recommend

We recommend that GSA's Federal Acquisition Service, Technology Transformation Services Director:

1. Revise the FedRAMP PMO's mission statement to a concise, singular statement.

2. Revise the FedRAMP PMO's objectives to make them more specific and measurable.

3. Review the FedRAMP PMO's mission, goals, and objectives to ensure they align in a cohesive manner.

The Federal Acquisition Service Commissioner agreed with the audit recommendations. GSA's written comments are included in their entirety as ***Appendix B***.

Table of Contents

Introduction

We performed an audit of GSA's Federal Risk and Authorization Management Program, (FedRAMP) Program Management Office's (PMO) goals and objectives.

Purpose

This audit was included in the GSA Office of Inspector General *Fiscal Year 2017 Audit Plan*. The initial focus was to review the authorization and accreditation process for third party providers who perform security assessments of cloud service providers (CSPs). However, during our audit survey, we determined that risks are present at the FedRAMP PMO level; therefore, we evaluated whether the FedRAMP PMO's goals and objectives are sufficient for assessing the effectiveness of the FedRAMP PMO in accomplishing its mission.

Objective

Our objective was to determine if the FedRAMP PMO's goals and objectives are sufficient to assess its effectiveness in accomplishing its mission.

See ***Appendix A*** – Scope and Methodology for additional details.

Background

On December 8, 2011, the Office of Management and Budget (OMB) issued *Security Authorization of Information Systems in Cloud Computing Environments,* which resulted in a collaborative effort between GSA and other federal entities, including the Departments of Defense and Homeland Security, to develop FedRAMP. FedRAMP is a government-wide program designed to increase the pace at which the federal government adopts cloud computing services. It was developed to standardize: (1) the process of how the Federal Information Security Management Act of 2002 (FISMA) applies to cloud computing services; and (2) the way the government conducts security assessments, authorizations, and continuous monitoring of cloud computing services.

FedRAMP has several key stakeholders:

(1) OMB: OMB has outlined the key components of FedRAMP and its operational capabilities. OMB is also responsible for defining the requirements for executive branch departments and agencies using FedRAMP, and providing oversight of the program.

(2) The Department of Homeland Security (DHS): Within FedRAMP's operational framework, DHS coordinates cybersecurity operations including incident response.

(3) The Joint Authorization Board (JAB): The JAB consists of the Chief Information Officers from the Department of Defense, DHS, and GSA. The JAB members define and update FedRAMP security authorization requirements in accordance with FISMA and DHS guidance, review authorization packages, and grant Provisional Authorities to Operate for cloud services.

(4) Executive branch departments and agencies: The executive branch departments and agencies are required to use FedRAMP when conducting risk assessments, reviewing security authorizations, and granting Authorities to Operate for use of cloud services.

(5) The FedRAMP PMO: The day-to-day operations of FedRAMP are performed by the FedRAMP PMO, which is managed by GSA's Federal Acquisition Service, Technology Transformation Services.

The FedRAMP PMO's responsibilities include:

- Creating a process for executive branch departments, agencies, and CSPs to adhere to FedRAMP security authorization requirements;
- Prioritizing authorization requests for JAB review;
- Establishing a centralized, secure repository of various authorization packages of cloud services that executive branch departments and agencies can leverage;
- Collaborating with the National Institute of Standards and Technology to develop and implement a program to accredit third-party assessment organizations to provide independent reviews of how CSPs implement the FedRAMP requirements; and
- Developing templates for executive branch departments and agencies to use to satisfy FedRAMP security authorization requirements.

Since the program began, government agencies and CSPs have expressed concerns regarding FedRAMP's efficiency, effectiveness, and transparency. They have noted that the Authority to Operate review and approval process is expensive and time consuming. A FedRAMP PMO official informed us that the PMO has been confronted with external pressures to speed up the FedRAMP process along with maintaining quality standards. While the FedRAMP PMO has taken action to address some of these concerns, additional action is needed to strengthen the PMO to better meet the needs and requirements of the program.

Results

The FedRAMP PMO's goals and objectives are not sufficient to assess if it is effectively accomplishing its mission. The FedRAMP PMO has not established an adequate structure comprising its mission, goals, and objectives for assisting the federal government with the adoption of secure cloud services. The mission statement does not provide a clear and concise direction for the FedRAMP PMO; objective statements are not specific and measurable; and the mission, goals, and objectives are not fully or accurately aligned which makes it difficult to determine if the FedRAMP PMO is meeting its mission effectively.

Finding 1 – The FedRAMP PMO's mission statement is not clear and concise, creating confusion regarding its main purpose.

The FedRAMP PMO does not have a single, clear and concise mission statement regarding its purpose. A mission statement is meant to set the tone of an organization defining its intentions and purpose. We found the FedRAMP PMO's mission statement to be a series of directives, which creates confusion regarding its main purpose.

According to OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget (2017*), a mission statement should be a brief, easy-to-understand narrative, usually no more than a sentence long. It should define the basic purpose of a program and be expressed in the broad context of a problem, need, or challenge. It enables employees to see how their work contributes to the broader mission and is a key component of a program's strategic plan, explaining why the program exists and what it does, while bringing the program into focus.

The FedRAMP PMO provided its mission statement, which encompasses multiple components derived from OMB memorandum, *Security Authorization of Information Systems in Cloud Computing Environments,* dated December 8, 2011. The FedRAMP PMO's mission is to:

- Reduce duplicative efforts, inconsistencies, and cost inefficiencies associated with the current security authorization process.
- Establish a public-private partnership to promote innovation and the advancement of more secure information technologies.
- Introduce an innovative policy approach to developing trusted relationships between executive branch departments and agencies and CSPs.
- Provide a cost-effective, risk-based approach for the adoption and use of cloud services by making available to executive branch departments and agencies:
    - Standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels.
    - A conformity assessment program capable of producing consistent independent, third-party assessments of security controls implemented by CSPs.
    - Authorization packages of cloud services reviewed by a JAB consisting of security experts from the DHS, Department of Defense, and GSA.

- Standardized contract language to help executive branch departments and agencies integrate FedRAMP requirements and best practices into acquisition.
- A repository of authorization packages for cloud services that can be leveraged government-wide.

The FedRAMP PMO's mission statement does not conform to the succinct format prescribed under OMB Circular No. A-11, but is rather a listing of directives established in the OMB memorandum. Therefore, the FedRAMP PMO's mission statement is not presented in a way that is focused or easily communicated, creating confusion as to its central purpose and vision of what needs to be accomplished. Accordingly, the FedRAMP PMO should establish a concise, clearly defined mission statement.

Finding 2 – The FedRAMP PMO's objective statements are not specific or measurable, impairing clarity and the ability to measure performance.

The FedRAMP PMO's objective statements are missing key attributes, hindering the understanding of what is to be accomplished and the effective communication of program results. Objective statements should be specific and measurable to assist in assessing performance.

In the *Standards for Internal Control in the Federal Government*, the U.S. Government Accountability Office defines various attributes of objectives.[1] Among other things, these standards provide that objectives should be:

- Defined in specific terms, such as what is to be achieved and how it will be achieved, so they are understood at all levels of the entity.
- Defined in measurable terms so that performance toward achieving those objectives can be assessed. Measurable objectives are generally free of bias and subjectivity.
- Supported by performance measures that are appropriate for evaluating the program's performance in achieving the objective.
- Aligned with the organization's mission, strategic plan, and performance goals.

The FedRAMP PMO established eight objectives to assess progress against its four goals, as listed below in *Figure 1*.

[1] GAO-14-704G, September 2014.

Figure 1 – FedRAMP PMO's Goals and Objectives

FedRAMP PMO Goal	FedRAMP PMO Objectives
More cloud to choose from	• Increase cloud services working with FedRAMP • Increase authorized cloud services • Establish FedRAMP Readiness as a viable readiness mechanism for CSPs
Transform security authorizations	• Ensure no authorizations take longer than 6 months • Launch FedRAMP Tailored • Redesign continuous monitoring
Stronger FedRAMP community	• Connect the community through industry and agency days • Promote better understanding
Maintain internal quality controls	*No corresponding objective provided*

The FedRAMP PMO's goals and objectives provided in *Figure 1* were documented in the FedRAMP PMO's Goal Tracker and published on its website. The goal tracker contained abbreviated objective statements intended to provide a convenient way for the public to view the goals, as well as the objectives and corresponding performance metrics at a glance. However, these simplified objective statements excluded information necessary for understanding and measuring the FedRAMP PMO's progress. Specifically, these objective statements were not defined in specific and measureable terms.

Objectives Not Defined in Specific Terms

We determined that some of the FedRAMP PMO's objective statements may not be easily understood by stakeholders and the public. For example, the FedRAMP PMO has two objectives that include similar language – "Increase cloud services working with FedRAMP" and "Increase authorized cloud services." These two objectives, as written, do not contain adequate detail to differentiate between them. While the FedRAMP PMO management team reviews its objectives internally on a routine basis, the difference between these objectives may not be evident or understood by those externally without further explanation. Vague objective statements may limit the understanding and clear communication of what the FedRAMP PMO strives to achieve.

Objectives Not Defined in Measurable Terms

We also found that some of the FedRAMP PMO's objective statements do not allow for a clear assessment of its performance. Many of the objectives do not explicitly identify a specific outcome, which would clearly outline what is to be achieved. For instance, the objective, "Promote better understanding" does not state what is to be understood or define how better understanding will be achieved. Similarly, "Establish FedRAMP Readiness as a viable readiness mechanism for CSPs" does not provide for clear measurement. The terms "viable" and "readiness" could be viewed as subjective and it is not clear from the objective how success will

be measured. While the FedRAMP PMO was able to provide us with some targets related to these objectives, the targets were not specifically outlined as part of its objectives. Objectives not defined in measurable terms negatively affect the FedRAMP PMO's ability to effectively communicate progress. Accordingly, the PMO should create objectives that are specific and measurable.

Finding 3 – The FedRAMP PMO's mission, goals, and objectives are not fully or accurately aligned, which inhibits the FedRAMP PMO's ability to assess its effectiveness.

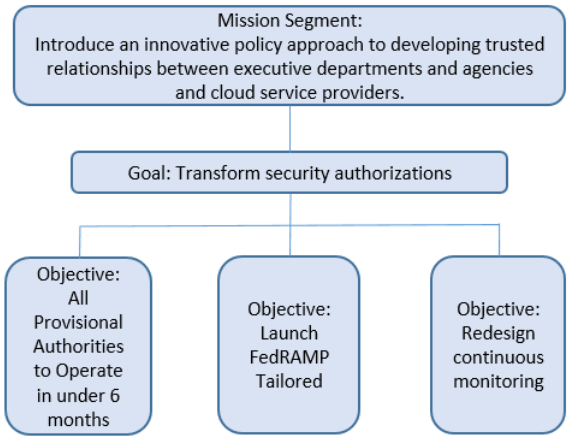
The FedRAMP PMO's mission, goals, and objectives do not align in a manner where its goals and objectives clearly support the mission. The lack of clear alignment of these elements inhibits the FedRAMP PMO's ability to assess its effectiveness in achieving its mission.

OMB Circular No. A-11 outlines the importance of aligning an organization's mission, goals, and objectives. An organization's mission directly supported and aligned with strategic goals, which are each supported and aligned with one or more strategic objectives, clearly outlines how each element is linked to the program's intended mission and purpose. When the FedRAMP PMO provided us with its goals and objectives, it clearly outlined how they were aligned; however, it did not include a connection to the specific mission statement segment. To evaluate the FedRAMP PMO's overall structure, we requested a document showing the alignment including the mission. The FedRAMP PMO provided us with this document, which aligned the mission, reported by mission segment, to the goals. From that document, we noted: (1) misalignments between mission segments and goals, and (2) mission segments and a goal without corresponding objectives.

Mission Segments and Goals Are Misaligned

Some of the FedRAMP PMO's mission segments and goals were misaligned. An example is depicted in *Figure 2* below.

Figure 2 – Misalignment of a Mission Segment and Goal

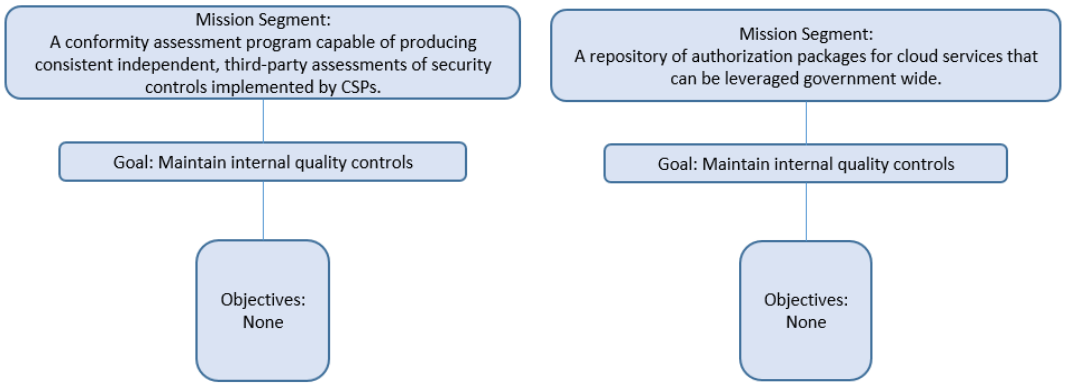


The mission segment "Introduce an innovative policy approach to developing trusted relationships between executive branch departments and agencies and cloud service providers" is aligned with the goal of "Transform security authorizations." This mission segment specifically focuses on relationships between government entities and CSPs. However, the goal of transforming security authorizations focuses more on increased efficiency of the process, not necessarily relationship building. To further demonstrate this, two of the three supporting objectives listed under this mission segment focus on increasing authorization efficiency rather than relationships between government entities and CSPs. Therefore, we determined that this mission segment and its corresponding goal are misaligned.

Mission Segments and Goal with No Supporting Objectives

We also noted that two of the FedRAMP PMO's mission segments and one goal do not have supporting objectives as shown below in *Figure 3.*

Figure 3 – Mission Segments and Goal with No Objectives



OMB Circular No. A-11 states that objectives should generally encompass the agency's mission and scope of responsibilities. Goals and objectives should directly support the program's mission. The lack of appropriate alignment among the FedRAMP PMO's goals, objectives, and mission inhibits the PMO's ability to assess its effectiveness in achieving its mission. Accordingly, the FedRAMP PMO should review its mission, goals, and objectives to ensure that they are aligned in a cohesive manner.

Conclusion

The FedRAMP PMO has not established an adequate structure comprising its mission, goals, and objectives for assisting the federal government with the adoption of secure cloud services. The FedRAMP PMO's mission statement does not provide a clear and concise direction, resulting in confusion regarding its central purpose and what needs to be accomplished. We also noted that some objective statements are not specific and measurable, which limits the understanding of what is to be accomplished and affects the FedRAMP PMO's ability to effectively communicate its progress. Further, we noted that the FedRAMP PMO's mission, goals, and objectives are not in alignment. Without the proper alignment of the mission, goals, and objectives, the FedRAMP PMO's ability to assess its effectiveness is inhibited. Accordingly, the FedRAMP PMO should review and revise its mission, goals, and objectives to ensure that they align in a cohesive manner to more effectively assess its progress and performance.

Recommendations

We recommend that GSA's Federal Acquisition Service, Technology Transformation Services Director:

1. Revise the FedRAMP PMO's mission statement to a concise, singular statement.

2. Revise the FedRAMP PMO's objectives to make them more specific and measurable.

3. Review the FedRAMP PMO's mission, goals, and objectives to ensure they align in a cohesive manner.

GSA Comments

The Federal Acquisition Service Commissioner agreed with the audit recommendations. GSA's written comments are included in their entirety as ***Appendix B***.

Audit Team

This audit was managed out of the Acquisition and Information Technology Audit Office and conducted by the individuals listed below:

Sonya D. Panzo	Associate Deputy Assistant Inspector General for Auditing
Michelle L. Westrup	Audit Manager
Bruce E. McLean	Auditor-In-Charge

Appendix A – Scope and Methodology

Our audit evaluated the FedRAMP PMO's mission, goals, and objectives.

To accomplish our objective, we:

- Reviewed existing federal laws, policy, and guidance governing FedRAMP, including:
  - OMB memorandum for Chief Information Officers, *Security Authorization of Information Systems in Cloud Computing Environments*, December 8, 2011;
  - *Guide to Understanding FedRAMP*, Version 2.0, June 6, 2014;[2] and
  - *FedRAMP Security Assessment Framework*, Version 2.4, November 15, 2017;[3]
- Reviewed information related to FedRAMP from GSA's intranet and FedRAMP's internet websites;
- Reviewed applicable criteria in assessing our results, including:
  - GAO-14-704G, *Standards for Internal Control in the Federal Government*, September 2014;
  - GAO-01-1008G, *Internal Control Standards, Internal Control Management and Evaluation Tool*, August 2001;
  - OMB Circular No. A-11, Preparation, Submission, and Execution of the Budget, July 2017;
  - GAO/AIMD/GGD-95-130R, *Goal-Setting and Performance*, March 1995;
  - GAO/GGD-10.1.16, *Agencies' Strategic Plans Under Government Performance and Results Act of 1993: Key Questions to Facilitate Congressional Review*, Version 1, May 1997;
  - 31 U.S.C. 1115, *Federal Government and agency performance plans*, 2015; and
  - Executive Order 13450, *Improving Government Program Performance*, November 2007; and
- Held discussions with FedRAMP PMO officials regarding their mission, goals, and objectives, to gain an understanding of FedRAMP.

We conducted the audit between October 2016 and May 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Internal Controls

Our assessment of internal controls was limited to those necessary to address the objective of the audit.

[2] The FedRAMP PMO developed this document.
[3] The FedRAMP PMO developed this document.

Appendix B – GSA Comments

GSA

GSA Federal Acquisition Service

February 14, 2019

MEMORANDUM FOR: Sonya D. Panzo
Associate Deputy Assistant Inspector General for Auditing
Office of Inspector General (J)

FROM: Alan B. Thomas, Jr.
Commissioner
Federal Acquisition Service (Q)

SUBJECT: Response to Discussion Draft *Audit of the Federal Risk and Authorization Management Program (FedRAMP), Program Management Office's (PMO's) Goals and Objectives*, Report Number A170023

Thank you for the Office of Inspector General's (OIG) draft report entitled *Audit of the Federal Risk and Authorization Management Program (FedRAMP), Program Management Office's (PMO's) Goals and Objectives (A170023)*, dated January 22, 2019. I appreciate the review of the FedRAMP PMO's mission, goals and objectives. The FedRAMP PMO is a top priority for the General Service Administration (GSA) Federal Acquisition Service (FAS) Office of Technology Transformation Services (TTS), as it is a government-wide program focused on the cybersecurity of cloud technology.

The FedRAMP PMO reviewed the OIG report and agrees with all of the recommendations. While we believe FedRAMP does have strong mission, goals, and objectives, we appreciate the OIG's recommendations for further clarity. We understand the importance of making these mission statements, goals, and objectives clearer for our stakeholders and the importance of strong accountability in measuring program effectiveness.

The FedRAMP mission was derived from multiple components within the Office of Management and Budget (OMB) FedRAMP Policy Memorandum, *Security Authorization of Information Systems in Cloud Computing Environments*, dated December 8, 2011. The FedRAMP PMO supports the OMB FedRAMP policy memorandum as stated and will develop a PMO-specific mission statement that is clear and concise to provide clarity to the program's stakeholders. Additionally, the PMO will refine its goals and objectives to ensure they are specific, measurable, and directly align to the program's mission.

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405

The FedRAMP PMO looks forward to working with the GSA OIG, and the opportunity to address the audit recommendations. If you have any questions, please contact Matthew Goodrich, Assistant Commissioner for the Office of Products and Programs at (202) 870-6231 or matthew.goodrich@gsa.gov.

Appendix C – Report Distribution

GSA Administrator (A)

GSA Deputy Administrator (AD)

Commissioner, Federal Acquisition Service (Q)

Acting Deputy Commissioner, Federal Acquisition Service (Q1)

Deputy Commissioner, Federal Acquisition Service/Technology Transformation Services Director (Q2)

Chief of Staff, Federal Acquisition Service (Q0A)

Senior Advisor, Federal Acquisition Service (Q0A)

Assistant Commissioner, Office of Policy and Compliance (QV)

Financial Management Officer, Federal Acquisition Service Financial Services Division (BGF)

Acting Assistant Commissioner, Office of Products and Programs (QX)

Acting FedRAMP Director (QXC)

Chief Administrative Services Officer (H)

Audit Management Division (H1EB)

Assistant Inspector General for Auditing (JA)

Director, Audit Planning, Policy, and Operations Staff (JAO)