NCUA
National Credit Union Administration

OFFICE OF INSPECTOR GENERAL

AUDIT OF THE NCUA'S CLOUD COMPUTING SERVICES

Report #OIG-24-01
February 12, 2024

SENT BY EMAIL

TO: Distribution List

FROM: Inspector General James W. Hagen

SUBJ: Audit of NCUA's Cloud Computing Services

DATE: February 12, 2024

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) conducted this self-initiated audit to assess the NCUA's use of cloud computing services. Our objectives were to determine whether the NCUA: (1) adequately addressed risk when contracting cloud computing services; and (2) effectively managed operational and security risks of implemented cloud computing services.

Results of our audit determined that the NCUA needs an enterprise-wide approach to cloud computing to effectively contract and manage cloud computing services. The NCUA should align policies and procedures with this enterprise-wide approach. Our audit also determined the NCUA implemented cloud computing services as the situation or business need occurred to meet mission priorities. We believe this approach has not allowed the NCUA to clearly address federal guidance, has created inconsistent processes, and allowed for decisions and implemented services to be made unsystematically. Therefore, we are making two recommendations in our report and note that management has agreed to both recommendations. Given the current approach to the agency's cloud computing services, the OIG plans to conduct a follow-up audit on the contracting and risk management of its use of cloud computing services once the recommendations in this report have been implemented.

We appreciate the cooperation and courtesies NCUA management and staff provided to us during the audit. If you have any questions on the report and its recommendation, please contact me at 703-518-6350.

Distribution:
Chairman Todd M. Harper
Vice Chairman Kyle S. Hauptman
Board Member Tanya Otsuka
Executive Director Larry Fazio
General Counsel Frank Kressman
Deputy Executive Director Rendell Jones
Chief of Staff Catherine D. Galicia
Office of External Affairs and Communication Elizabeth Eurgubian
Chief Information Officer Robert Foster
Senior Agency Information Security/Risk Officer William D. Tillman

Associate General Counsel for Information and Access Law Elizabeth Harris
Office of Business Innovation Director Amber Gravius
Chief Financial Officer Eugene Schied
Director Division of Procurement Facilities Management John Ziu

Attachment

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) conducted this self-initiated audit to assess the NCUA's Cloud Computing Services. Our objectives were to determine whether the NCUA: (1) adequately addressed risk when contracting cloud computing services; and (2) effectively managed operational and security risks of implemented cloud computing services. The scope of our audit covered cloud computing services from June 1, 2021, through June 1, 2023.

Our audit determined that the NCUA needs an enterprise-wide approach to cloud computing to effectively contract and manage cloud computing services. Additionally, the NCUA should align policies and procedures with the enterprise-wide approach. Our audit also determined the NCUA implemented cloud computing services as the situation or business need occurred. This approach, we believe, has not allowed the NCUA to clearly address federal guidance, has created inconsistent processes, and allowed for decisions and implemented services to be made unsystematically.

We are making two recommendations in our report to address the issues identified. Given the current approach to NCUA's cloud computing services, the OIG plans to conduct a follow-up audit on the contracting and risk management of NCUA's use of cloud computing services once the recommendations in this report have been implemented.

We appreciate the cooperation and courtesies NCUA management and staff provided to us during this audit.

BACKGROUND

The NCUA is an independent federal agency created by the U.S. Congress that insures deposits of federally insured credit unions, protects members who own credit unions, and charters and regulates federal credit unions. The NCUA's organizational structure consists of a Headquarters in Alexandria, Virginia, an Asset Management and Assistance Center in Austin, Texas, and three regional offices[1] that carry out the agency's supervision and examination program.

The NCUA's contracting and management of implemented cloud computing services is coordinated between multiple offices, which includes the Office of Business Innovation (OBI), Office of the Chief Information Officer (OCIO), Office of the Chief Financial Officer (OCFO), Office of General Counsel (OGC), and the office of primary interest (OPI).

Cloud Computing Defined

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-144, *Guidelines on Security and Privacy in Public Cloud Computing* defines cloud computing as:

> A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

In cloud computing environments, some controls over information assets and operations may be outsourced to a Cloud Service Provider (CSP). A careful review of the contract between the agency and the CSP, along with an understanding of the potential risks, are important in management's understanding of its responsibilities for implementing appropriate controls. Failure to understand the division of responsibilities for assessing and implementing appropriate controls over operations may result in increased risk of operational failures or security breaches. Processes should be in place to identify, measure, monitor, and control the risks associated with cloud computing.

Cloud computing models deliver services at varying levels of responsibility, which may also differ between CSPs per contract. The three most used service models are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS typically delivers software applications by subscription from a CSP. The CSP fully manages the application and customer responsibilities are generally limited to data ownership and access management. PaaS provides additional functions by offering a platform where software can be developed, managed, and deployed. The customer is responsible for applications developed on the platform, but the CSP maintains primary responsibility over the cloud infrastructure. IaaS

[1] The three regional offices are the Eastern, Southern, and Western regions.

provides the customer direct access to infrastructure with scalability. It is the most flexible of the models with also the greatest customer responsibility as the customer is responsible for anything they own or install on the cloud infrastructure.

Federal Laws, Guidance, and Policy related to Cloud Computing

In 2011, the Federal Government began its push for agencies to adopt cloud computing with the Office of Management and Budget's (OMB's) *Federal Cloud Computing Strategy*. This "Cloud First" strategy eventually became restructured as "Cloud Smart" in 2019.[2] The "Cloud Smart" strategy aimed to accelerate adoption of cloud-based solutions by focusing on addressing security, procurement, and workforce requirements. Additionally, the development of the Federal Risk and Authorizations Management Program (FedRAMP)[3] was designed to promote secure cloud adoption by the Federal Government through standardizing security requirements for authorization and allowing for agencies to leverage shared authorization packages in the FedRAMP marketplace. In December 2022, the FedRAMP Authorization Act[4] codified the FedRAMP program as the authoritative approach for federal cloud computing services and provides for formal reciprocity by allowing agencies to reuse Authorizations to Operate (ATOs) under a "presumption of adequacy." Agencies may reuse ATOs to the extent practicable but establish specific security control and contractual requirements[5] based on the agency's security posture and mission needs. In October 2023, OMB provided a draft for public comment on a memo modernizing FedRAMP that would replace the 2011 memorandum.[6]

In May 2021, Executive Order 14028 called upon federal agencies to define and implement cloud-based infrastructure to support zero-trust strategy. Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.[7] Instead of traditional security tied to a network perimeter, zero-trust architecture protects each file, email, and network by authenticating every identity and device. The zero-trust security model assumes threats exist inside and outside network boundaries that must be constantly scanned for, it also limits access to only those who need it. Cloud computing services support the implementation of a zero-trust strategy because configuration and management requirements within the cloud can adhere to the zero-trust model.

Several OMB directives have been issued that consider or address the use of cloud computing services including OMB 19-03, *Management of High Value Assets*, OMB 22-09, *Federal Zero Trust Strategy*, and OMB 22-18, *Enhancing the Security of the Software Supply Chain*. While

[2] Office of the Federal Chief Information Officer, Federal Cloud Computing Strategy (June 2019).
[3] OMB Memorandum for Chief Information Officers, Security Authorizations of Information Systems in Cloud Computing Environments (Dec. 8, 2011).
[4] FedRAMP Authorization Act, 44 U.S.C. §§ 3607-16.
[5] FedRAMP Control Specific Contract Clauses (Dec. 8, 2017).
[6] Draft Modernizing the Federal Risk Authorization Management Program (FedRAMP), (Oct. 27, 2023)
[7] NIST Special Publication 800-207 Zero Trust Architecture (August 2020).

these directives are not specific to only cloud computing, they highlight the broad considerations necessary when implementing cloud computing services.

NCUA's Cloud Computing Services

As of November 2023, the NCUA utilizes 58 cloud computing services, which include 3 IaaS, 51 SaaS, and 7 PaaS. Three systems are used in both a SaaS and PaaS capacity. Cloud computing services are procured through the NCUA's acquisition process, which follows the Acquisition Policy Manual (APM) and are authorized for use through the NCUA's Assessment and Authorization (A&A) process.

Contracting of Cloud Computing Services

The NCUA's APM, dated December 2019, establishes the procurement policy of the NCUA, which applies to all acquisitions of goods and services by the agency, including cloud computing services, which falls under information technology.[8] Section 2.106 of the APM identifies that the acquisition of information technology (IT) requires approval by the Chief Information Officer or designee.

The APM also includes a specific clause for cloud managed services: 9.500-2, *Cloud Managed Services*. This clause is expected to be inserted in every cloud service procurement, as determined by OCIO. The clause defines managed services, includes FedRAMP requirements, and addresses compliance reviews, data jurisdiction, system security and continuous monitoring plans, and physical security.[9] The clause requires the OCIO to select the type of cloud service provider when addressing documentation requirements:

1. Joint Accreditation Board (JAB)-certified[10] CSP.
2. Cloud computing services from an agency-certified CSP.[11]
3. Cloud computing services from a contractor that is not a FedRAMP certified CSP.

Non-FedRAMP certified CSPs are expected to maintain documentation using current requirements of NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.

When an OPI requests an IT service which may include the use of a cloud service provider, the following offices have responsibilities related to the procurement and risk management of the service:

[8] APM (Rev. 3) was published on December 14, 2023.
[9] APM (Rev. 3) also includes a clause for supply chain risk.
[10] The JAB is the primary governance and decision-making body for FedRAMP.
[11] APM (Rev. 3) clarified this statement to be an agency-certified FedRAMP CSP or subscription.

- OBI – OBI provides the Information System Security Officer (ISSO) who serves as the principal advisor to the OPI's system owner and develops documentation needed for the security authorization.

- OCIO – OCIO's Information & Technology Assurance Division addresses the technical and cybersecurity risks of implementation and provides approval as part of the security authorization.[12]

- OCFO – OCFO's Division of Procurement and Facilities Management supports the procurement of IT services through the acquisition process defined in the APM.

- OGC – OGC's Information and Access Law Division addresses the legal and privacy risk of implementation and provides approval as part of the security authorization.

NCUA's Security Authorization of Information Systems

In July 2020, the NCUA issued a revision to A&A Standard Operating Procedure (A&A SOP).[13] NCUA issued the A&A SOP to guide the implementation of the risk management framework for NCUA information systems and services. A security authorization is the official management decision given by a senior organizational official to authorize operation of an information system and explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security controls. The NCUA's CIO is the agency's senior organizational official who authorizes operations of NCUA's information systems. The OPI follow the NCUA A&A process for obtaining a security authorization for their systems.

An information system must be granted an ATO before it becomes operational and re-authorized every 3 years or whenever a significant change is made that affects the potential risk level of operating the system. Ongoing authorizations may be allowed to extend ATOs beyond 3 years. Services that are utilized by the agency must be granted an Authorization to Use (ATU) after a review of the security posture of the service provider to determine appropriate security controls are in place.

The A&A process allows for the following systems:

1. NCUA-hosted systems and NCUA-sponsored contractor systems subjected to Federal Information Security Management Act (FISMA) requirements.

2. Any FedRAMP-authorized systems or services.

[12] APM (Rev. 3), states that NCUA Chief Information Officer (CIO) and Senior Information Security/Risk Officer bear the primary responsibility to ensure compliance with NIST, OMB, and all applicable laws, directives, policies, and directed actions on a continuing basis.
[13] Version 3.2 dated July 16, 2020.

3. U.S. government agency-authorized systems or services.

4. Cloud-based or contractor run systems not following FISMA (e.g., those that utilize AICPA SOC, or ISO attestation) and do not meet the requirements of 1-3.

Options 1-3 follow NIST SP 800-37, *NIST Risk Management Framework* which uses NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations* controls. Option 4 relies on System & Organization Controls (SOC) attestation report based on Statement on Standards for Attestation Engagements (SSAE) No. 18 (either Type 1 or Type 2), NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, or International Organization for Standardization (ISO) 27001.

RESULTS IN DETAIL

The objectives of our audit were to determine whether the NCUA: (1) adequately addressed risks when contracting for cloud computing services; and (2) effectively managed operational and security risks of implemented cloud computing services. The detailed results of our audit follow.

The NCUA Needs an Enterprise-Wide Approach to Cloud Computing

We determined that the NCUA did not document and formalize a comprehensive enterprise-wide approach to cloud computing that was consistent with federal requirements and guidance. Specifically, NCUA management should address the prioritization of FedRAMP-authorized cloud computing services and align policies and processes with federal guidance such as OMB's Federal Cloud Computing Strategy. In addition, NCUA management should clearly establish roles, responsibilities, and practices related to the technical reviews in the procurement of IT services, which include cloud computing services. The lack of an enterprise-wide approach occurred because NCUA management contracted and managed cloud computing services in an ad-hoc manner.[14] As a result, the agency's approach does not clearly address federal guidance, includes inconsistent processes, and allows for cloud computing decisions to be implemented unsystematically.

We believe establishing and implementing an enterprise-wide cloud computing approach aligned with federal guidance would improve the NCUA's ability to effectively manage cloud computing risk. In addition, implementing policies and procedures consistent with this enterprise-wide approach would enhance internal coordination among stakeholders, increase operational efficiency, and reduce costs to the NCUA and the burden on vendors.

Given the lack of an enterprise-wide approach to cloud computing, we deferred evaluation of strategy implementation and specific system testing until management has established a strategy and implemented policies, procedures, and processes that align. The OIG plans to follow-up on the contracting and risk management of the NCUA's use of cloud computing services once the recommendations in this report have been implemented.

Details

We determined that the NCUA's contracting, and risk management of cloud computing services could be improved through a formalized enterprise-wide approach to cloud computing. Specifically, we determined:

- NCUA management did not have a documented enterprise-wide cloud computing strategy in place[15] that was implemented within the agency across all stakeholder offices.

[14] For example, when agency officials moved staff to full-time remote work during the COVID-19 pandemic and required access to cloud services or when management identified a specific business need.
[15] On January 3, 2024, OCIO disseminated a draft cloud strategy for agency review.

Instead, the agency's approach has been to address cloud computing services ad-hoc through leveraging and contracting various cloud solutions to meet specific mission priorities.

- NCUA management does not have formal criterion in place on when to leverage cloud computing services and how to determine which service(s) to use. This limits appropriate planning for cloud computing services.

- The NCUA did not have a policy that specifically prioritized FedRAMP-authorized cloud computing services or clearly addressed when an alternative would be suitable. The NCUA predominantly used non-FedRAMP-authorized services. We determined 41 out of 58 (70 percent) of the NCUA's cloud computing services were not FedRAMP-authorized and the NCUA instead relied on ATOs or ATUs utilizing attestations identified in the NCUA A&A process. Although the NCUA's OCIO recognized the benefit of FedRAMP from a cost, consistency, and ease of service perspective, the OCIO focused their efforts on managing risk regardless of FedRAMP authorization. We learned the OCIO did this to allow for more contracting options.

- The NCUA did not comprehensively align internal processes to OMB's Federal Cloud Computing Strategy (Cloud Smart), which includes improved practices on security, procurement, and workforce planning. For example, although we determined the NCUA did not have standardized service-level agreements for cloud service contracts, we determined the agency informally identified that improvements could be made to cloud architecture and data governance to increase the maturity of NCUA's cloud implementation.

- NCUA management did not clearly define roles, responsibilities, and practices related to the technical reviews in the contracting of IT services, including cloud computing services. During the contracting process, the workflow of NCUA stakeholder reviews was not clearly identified and documentation requirements for vendors were not transparent. Given the number of offices (OBI, OCIO, OCFO, OGC, and OPI) involved with contracting for IT services, we believe clear expectations for each office and requirements for vendors would increase coordination within the NCUA and reduce burden on vendors.

- NCUA officials were unable to provide us with a complete listing of every cybersecurity and operational incident affecting cloud computing services for the scope period of our audit. This was due to how OCIO categorized and recorded incidents. However, through interviews with staff, we were able to identify incidents that showed improvements in risk management might be needed. In addition, we determined at least one cybersecurity incident of a cloud computing system occurred during the scope period of our audit. Specifically, NCUA staff and contractors responsible for overseeing a contractor owned system did not timely report an incident within the agency's ticketing system, nor did they effectively communicate the incident to the proper officials within the NCUA.

Based on the issues identified above, we are making the following recommendations.

Recommendations

We recommend NCUA management:

1. Finalize and implement a comprehensive formalized enterprise-wide cloud computing strategy that, at minimum, addresses the following:

    - Alignment with federal guidance and directives such as Cloud Smart and Executive Order 14028.
    - Prioritization of the use of FedRAMP-authorized systems.
    - Identification of workforce requirements needed to support cloud procurement, implementation, and risk management.
    - Management of risks related to the use of cloud computing services such as secure cloud architecture, data governance, and incident management processes.

Management Response

Management agreed with the recommendation. Management indicated they began working on a cloud strategy after Executive Order 14028 was issued and expect to finalize it no later than December 31, 2024.

OIG Response

We concur with management's planned action.

2. Develop and implement policies, procedures, and standards that are consistent with the NCUA's cloud computing strategy and address, at minimum, the following:

    - Coordination, identification, and clarification of responsibilities and processes across all stakeholders for IT service contract reviews, service-level agreements alignment and monitoring, and cloud service incident management.
    - Specific criterion for the prioritization, selection, and use of cloud computing services.
    - Periodic review of contract clauses included for cloud computing services to confirm documentation supporting security requirements are clearly identified to the vendor and security and operational risks are appropriately managed.

Management Response

Management agreed with the recommendation. Management indicated they plan to develop, update, and implement policies, procedures, and standards, consistent with the approved cloud computing strategy by June 30, 2025.

OIG Response

We concur with management's planned actions.

Appendix A

OBJECTIVE, SCOPE, AND METHODOLOGY

We developed our objectives for this engagement based on OIG's 2023 Annual Work Plan. Specifically, our objectives were to determine whether the NCUA: (1) adequately addressed risks when contracting for cloud computing services and (2) effectively managed operational and security risks of implemented cloud computing services.

To accomplish our audit, we performed fieldwork with information relevant to NCUA's use of cloud computing services between June 2023 through January 2024.

The scope included cloud computing services provided to NCUA from June 1, 2021, through June 1, 2023. To achieve our objective, we performed the following:

- Identified and reviewed federal guidance and requirement for cloud computing services.
- Conducted interviews with NCUA staff and management with contracting and risk management responsibilities related to cloud computing services.
- Evaluated NCUA policies and procedures related to procurement and risk management of cloud computing services.
- Evaluated internal controls.

Due to the lack of an enterprise-wide approach to cloud computing at the NCUA, the OIG modified the audit methodology to not include evaluation of strategy implementation and specific system testing until a strategy has been established and policies and procedures aligned. We did not significantly rely on computer-processed data to answer the audit objectives. Although we obtained a cloud system inventory and reviewed incidents generated from NCUA systems, these were not significant to the objectives themselves. Therefore, we did not test controls over these systems. Rather, we relied on our analysis of information from interviews, policies, and procedures to evaluate the data and support our audit conclusions. The OIG plans to follow-up on the contracting and risk management of NCUA's use of cloud computing services once the recommendations in this report have been implemented.

We conducted this audit from June 2023 through January 2024 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. 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 objectives. We assessed the effectiveness of the internal controls and determined they were significant to the audit objective. Specifically, we assessed 5 of the 5 internal control Components and 12 of the 17 associated

underlying Principles defined in the Government Accountability Office's Standards for Internal Control in the Federal Government.[16]

We summarize in Table 1 below the components and principles we assessed.

Table 1: Internal Control Components and Underlying Principles Assessed

Component: Control Environment	
	Principle 3 - Establish Structure, Responsibility, and Authority
	Principle 4 - Demonstrate Commitment to Competence
Component: Risk Assessment	
	Principle 6 - Define Objectives and Risk Tolerance
	Principle 7 - Identify, Analyze, and Respond to Risks
	Principle 9 - Identify, Analyze, and Respond to Change
Component: Control Activities	
	Principle 10 - Design Control Activities
	Principle 11 - Design Activities for the Information System
	Principle 12 - Implement Control Activities
Component: Information and Communication	
	Principle 13 - Use Quality Information
	Principle 14 – Communicate Internally
Component: Monitoring	
	Principle 16 – Perform Monitoring Activities
	Principle 17 – Evaluate Issues and Remediate Deficiencies

The report presents within the findings the internal control deficiency we identified. However, because our audit was focused on these significant internal controls, Components, and underlying Principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

[16] The Standards for Internal Control in the Federal Government organizes internal control through a hierarchical structure of 5 components and 17 principles. The five components, which represent the highest level of the hierarchy, consist of the Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring. The 17 principles support the effective design, implementation, and operation of the components, and represent the requirements for establishing an effective internal control system.

Appendix B

NCUA MANAGEMENT RESPONSE

National Credit Union Administration
Office of the Executive Director

SENT VIA EMAIL

TO: Inspector General James Hagen

FROM: Executive Director Larry Fazio

SUBJ: Management Response- *Audit of the NCUA's Cloud Computing Services*

DATE: February 08, 2024

We reviewed the Office of the Inspector General's draft audit report titled *Audit of the NCUA's Cloud Computing Services*. We agree with the two recommendations.

Recommendation 1:
Finalize and implement a comprehensive formalized enterprise-wide cloud computing strategy that, at minimum, addresses the following:

- Alignment with federal guidance and directives such as Cloud Smart and Executive Order 14028.
- Prioritization of the use of FedRAMP-authorized systems.
- Identification of workforce requirements needed to support cloud procurement, implementation, and risk management.
- Management of risks related to the use of cloud computing services such as secure cloud architecture, data governance, and incident management processes.

Management Response: We agree with this recommendation. The NCUA began working on a cloud strategy after Executive Order 14028 was issued. The NCUA's draft cloud computing strategy is undergoing review, and we expect to finalize the strategy no later than December 31, 2024.

Recommendation 2:
Develop and implement policies, procedures, and standards that are consistent with the NCUA's cloud computing strategy and address, at minimum, the following:

- Coordination, identification, and clarification of responsibilities and processes across all stakeholders for IT service contract reviews, service-level agreements alignment and monitoring, and cloud service incident management.
- Specific criterion for the prioritization, selection, and use of cloud computing services.
- Periodic review of contract clauses included for cloud computing services to confirm documentation supporting security requirements are clearly identified to the vendor and security and operational risks are appropriately managed.

1775 Duke Street – Alexandria, VA 22314-6113 – 703-518-6320

Page 2

Management Response: We agree with this recommendation. The NCUA will develop, update, and implement policies, procedures, and standards, consistent with the approved cloud computing strategy no later than June 30, 2025.

Thank you for the opportunity to comment on the draft report.

Appendix C

ACRONYMS AND ABBREVIATIONS

Acronym	Term
A&A	Assessment and Authorization
APM	Acquisition Policy Manual
ATO	Authorization to Operate
ATU	Authorization to Use
CIO	Chief Information Officer
CSP	Cloud Service Provider
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
IaaS	Infrastructure as a Service
ISO	International Organization for Standardization
ISSO	Information System Security Officer
IT	Information and Technology
JAB	Joint Accreditation Board
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
OBI	Office of Business Innovation
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OGC	Office of General Counsel
OPI	Office of Primary Interest

Acronym	Term
OMB	Office of Management and Budget
PaaS	Platform as a Service
SaaS	Software as a Service
SOC	System and Organization Controls
SOP	Standard Operating Procedure
SP	Special Publication
SSAE	Statement on Standards for Attestation Engagements