



Office of Inspector General Best Practices for Cloud Computing

March 2026

PREFACE

This white paper presents best practices that Federal Offices of Inspectors General (OIGs) can use to plan, implement, and report on their agency's cloud computing activities. It is not intended to be policy or a substitute for professional judgment. OIGs may integrate the elements outlined in this document into the relevant standards applicable to their work.

Table of Contents

Background and Objective	1
Objective	1
Cloud Computing Technology	2
Criteria for Federal Agencies.....	2
Cloud Service Models.....	3
Governance	5
Best Practice 1: Reviewing all contracts will ensure appropriate clauses are in place to define roles and responsibilities.	5
Best Practice 2: Reviewing the governance framework will ensure policies, procedures, and responsibilities are in place to maximize security, operating efficiency, and compliance with regulatory requirements.	6
Risk	7
Best Practice 3: Reviewing service agreements ensures risk mitigation measures have been agreed upon.	7
Compliance	8
Best Practice 4: Reviewing artifacts will ensure CSPs and agencies comply with security and performance expectations.....	8
Common Security Controls	9
Best Practice 5: Assessing roles and privileges will identify if roles are appropriately granted and in accordance with common security practices, such as the least privilege principle.	10
Best Practice 6: Assessing data requirements will identify what data is allowed to be stored in the cloud.....	11
Best Practice 7: Assessing configuration settings will provide assurance that the system is configured according to the agency’s operational requirements.....	12
Best Practice 8: Ensuring audit logs are maintained and reviewed will provide visibility into identified vulnerabilities and threats.	12
Best Practice 9: Determining if the agency has complete and up-to-date information regarding their cloud inventory will ensure the agency does not have shadow IT.....	13
Appendix 1-Sample Audit Plan.....	14
Appendix 2-Example OIG Reports.....	18
Appendix 3-Key Terms and Definitions.....	22
List of Contributors	24



Background and Objective

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) was statutorily established as an independent entity within the executive branch by the [Inspector General Reform Act of 2008](#), Public Law 110-409. The mission of CIGIE is to:

- Address integrity, economy, and effectiveness issues that transcend individual government agencies; and
- Increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the Federal Inspector General (IG) community.

Within the CIGIE, the Federal Audit Executive Council's (FAEC) purpose is to discuss and coordinate issues affecting the federal audit community with special emphasis on audit policy and operations of common interest to members. The scope and activities of the FAEC include, but are not limited to, issuing guidance on the external Peer Review Process; coordinating joint audit projects; providing input on policies related to Federal Government audits; and coordinating with the Government Accountability Office, Office of Management and Budget (OMB), and others on matters affecting audit policy. The FAEC reports to the Audit Committee of the CIGIE, and other organizations as deemed appropriate.

The FAEC formed a working group to research and identify best practices for Offices of Inspectors General (OIGs) in performing assessments of an agency's cloud computing environment. This report was prepared by representatives from three participating OIGs.¹ The working group reviewed prior OIG cloud computing reports ([See Appendix 2](#)) and researched common industry standards and best practices to develop key considerations for planning and executing reviews of the management and implementation of cloud computing environments. It is important to note that the information presented in this document represents a point-in-time and as technology advances, policies and best practices will continue to evolve. The guidance in this white paper is not prescriptive; each OIG should use professional judgment in assessing the agency's implementation and security of cloud computing environments. OIGs may integrate the elements outlined in this document into the relevant standards applicable to their work (e.g. Government Accountability Office (GAO) [Generally Accepted Government Auditing Standards](#) (Yellow Book), CIGIE [Quality Standards for Inspection and Evaluation](#) (Blue Book), etc.)

Objective

The objective of the FAEC cloud computing working group was to identify best practices for OIGs in performing assessments of an agency's cloud computing environment.

¹ United States Postal Service (USPS) OIG, Federal Deposit Insurance Corporation (FDIC) OIG, and United States Agency for International Development (USAID) OIG.

Cloud Computing Technology

Cloud computing is the delivery of computing services – including servers, storage, databases, networking, software, analytics, and intelligence – over the internet to offer faster innovation, flexible resources, and economies of scale.² For over a decade, federal agencies have increasingly used cloud computing to address their information technology (IT) needs and to perform their missions. Cloud computing offers federal agencies a means to buy services quicker and at a potentially lower cost than building, operating, and maintaining these computing resources themselves.

Criteria for Federal Agencies

In recent years, the federal government has issued requirements and guidelines for protecting an agency's cloud computing environment. Most recently, on June 6, 2025, the Administration released Executive Order 14306, *Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144*.³ Among other cybersecurity priorities, the order continued the emphasis on securing Government cloud services within Federal information systems. At the forefront of these efforts to implement secure cloud computing environments are policies issued by the OMB. For example, in June 2019, OMB published the [Federal Cloud Computing Strategy](#) (also known as Cloud Smart), which provides actionable guidance to assist agencies with the secure adoption of cloud-based technologies. With agencies modernizing their environments, cloud security becomes a larger focus for OIGs across the federal government. OIGs should ensure that their agency's cloud environment and data are protected, and that the agency follows security best practices.

Further, the OMB published a revised policy memorandum⁴ on July 25, 2024, that includes an updated vision, scope, and governance structure for the Federal Risk and Authorization Management Program (FedRAMP), with the goal to strengthen and enhance the program. The purpose of FedRAMP is to increase federal agencies' adoption and secure use of the commercial cloud by providing a standardized, reusable approach to security assessments and authorizations for cloud computing products and services. FedRAMP's goal is to ensure that Federal information systems and information continue to be protected, even when the agency that owns those systems and information does not have complete control over them. To achieve this, FedRAMP has several strategic goals and responsibilities, including: (1) leading an information security program grounded in technical expertise and risk management, (2) rapidly increasing the size of the FedRAMP Marketplace by evolving and offering additional FedRAMP authorization paths, (3) streamlining processes through automation, and (4) leveraging shared infrastructure between the federal government and private sector. On March 24, 2025, the U.S. General Services Administration (GSA) announced [FedRAMP 20x](#), a pilot approach to accelerate

² Microsoft Azure, [What is cloud computing?](#).

³ This document reflects amendments resulting from this guidance.

⁴ OMB Memorandum for the Heads of Executive Departments and Agencies, [Modernizing the Federal Risk and Authorization Management Program \(FedRAMP\)](#) (July 25, 2024). This rescinds the original memorandum, OMB Memorandum for Chief Information Officers, [Security Authorization of Information Systems in Cloud Computing Environments](#) (December 8, 2011).

cloud adoption. Two of the four core principles of FedRAMP 20x include making it easier for cloud service providers (CSP)⁵ to follow modern security practices and streamlining security requirements to expedite the approval of cloud services.

While these requirements may not be applicable to agencies outside the executive branch, broader criteria exist that may be applied while leveraging the best practices identified in this document. For example, the GAO [Standards for Internal Control in the Federal Government](#) (Green Book), dated September 2024, sets internal controls standards for Federal agencies. The standards require management to design information systems and related control activities to meet objectives and address risks. Management should continue to evaluate changes in the use of IT and design new control activities when these changes are incorporated into the agency's IT infrastructure. These control activities include security management, logical access, and configuration management.

Cloud Service Models

There are three main cloud service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Each model has a unique mix of shared responsibility that will drive whether the CSP or the agency owns the security tasks and functions ([See Figure 1](#)).

- With IaaS, the CSP owns the security tasks for facility, data centers, and network components, while the agency owns security for host operating systems that run the applications and code. The agency can then provision processing, storage, networks, and other fundamental computing resources to deploy and run software, such as operating systems and applications.
- With PaaS, ownership is to some extent a middle ground. The agency has more responsibility than it would using SaaS, but less than if it were to use IaaS. Under this model, the CSP owns the security for the same components as IaaS and the guest operating system, while the agency has ownership of application and data security controls.
- With SaaS, the agency has the least amount of responsibility. The CSP owns the security tasks for the physical, infrastructure and application-level controls. But the agency is still responsible for security of its data and access to that data.

⁵ A third-party company that provides scalable computing resources that businesses can access on demand over a network, including cloud-based compute, storage, platform, and application services. Retrieved from Google Cloud, [What is a cloud service provider?](#).

FIGURE 1: Cloud Service Models



Source: Microsoft Azure and National Institute of Standards and Technology (NIST) SP 800-145.

With the adoption of cloud computing comes unique risks to these types of environments. Agencies are usually responsible for access controls to the cloud system. However, some controls are the responsibility of the CSP. For example, the CSP is responsible for some of the security controls related to incident or patch management. At the same time, some agreements may not require CSPs to provide such services, leaving a gap in security defenses. Therefore, it is important for agencies to have a governance, risk, and compliance framework⁶ in place to appropriately assess and respond to risks and provide assurance in the cloud environment, especially as it relates to security. Governance, risk, and compliance ensures data security, system integration, and the deployment of cloud computing are properly managed. OIGs need to be aware of an agency’s understanding and implementation of governance, risk, and compliance, as this is critical to assessing cloud security controls.

The FAEC working group identified nine best practices aligned to the areas of governance, risk, compliance, and relevant security controls. These best practices are designed to assist OIGs in performing their assessments of an agency’s cloud computing environment. See [Table 1](#) for the best practices as they align to each area of consideration. Additionally, the working group developed a sample audit plan to guide OIGs in planning assessments aligned with these best practices (See [Appendix 1](#)).⁷

Table 1: Best Practices for Assessing an Agency’s Cloud Computing Environment

Consideration Area	Best Practice
Governance	<ol style="list-style-type: none"> 1) Reviewing all contracts will ensure appropriate clauses are in place to define roles and responsibilities. 2) Reviewing the governance framework will ensure policies, procedures, and responsibilities are in place to maximize

⁶ Governance, risk, and compliance helps organizations align information technology activities to business goals, manage risk effectively, and stay in compliance with government and industry regulations. Governance includes the policy, process, and internal controls that comprise how an organization is run.

⁷ Some agencies may hire a managed service provider (MSP) to help manage their cloud-based resources and infrastructure. In this case, the MSP is responsible for ensuring compliance with the agency’s security and performance expectations. However, the agency is still responsible for governance and oversight of the MSP to ensure agency objectives are met.

	security, operating efficiency, and compliance with regulatory requirements.
Risk	3) Reviewing service agreements will ensure risk mitigation measures have been agreed upon.
Compliance	4) Reviewing artifacts ⁸ will ensure CSPs and agencies comply with security and performance expectations.
Security Controls	<p>5) Assessing roles and privileges will identify if roles are appropriately granted and in accordance with common security practices, such as the least privilege principle.</p> <p>6) Assessing data requirements will identify what data is allowed to be stored in the cloud.</p> <p>7) Assessing configuration settings will provide assurance that the system is configured according to the agency's operational requirements.</p> <p>8) Determine if the agency maintains and reviews audit logs⁹ will provide visibility into identified vulnerabilities and threats.</p> <p>9) Determining if the agency has complete and up-to-date information regarding their cloud inventory¹⁰ will ensure the agency does not have shadow IT.¹¹</p>

Source: FAEC Working Group.

Governance

A cloud governance¹² framework ensures cloud operations are secure as it provides a plan for the implementation of common security controls. Cloud computing impacts an agency's governance for one of two reasons: (1) it introduces a third-party into the process when leveraging cloud services provided by a CSP, or (2) it can potentially alter an agency's internal governance structure if the cloud service is hosted by the agency. The most important consideration for any agency that is using or considering using cloud computing is that the agency can never outsource its responsibility for governance, even if using a third-party.

Best Practice 1: Reviewing all contracts will ensure appropriate clauses are in place to define roles and responsibilities.

The primary tool an agency uses for governance is the contract that it has with the CSP. The contract is what is going to guarantee the level of service an agency can be expected to receive from a CSP, so it's vital that appropriate agreements are put in place. This includes defining

⁸ Artifacts are logs, documentation, or other materials used to support compliance activities.

⁹ An audit log is defined as a chronological record of system activities, including records of system accesses and operations performed in a given period.

¹⁰ A cloud inventory is a detailed record of all the resources and assets within an organization's cloud environment.

¹¹ Shadow IT refers to IT systems, devices, software, or applications used within an agency without the IT department's approval or oversight.

¹² Cloud governance is a set of policies and rules used by agencies while they build or work in the cloud environment.

roles and responsibilities, implementing change management processes, establishing service-level agreements, and conducting regular audits to ensure adherence to governance standards.

Best Practice 2: Reviewing the governance framework will ensure policies, procedures, and responsibilities are in place to maximize security, operating efficiency, and compliance with regulatory requirements.

To effectively manage their cloud environments, agencies should develop governance practices that align with their business objectives and regulatory requirements. The following industry standards for cloud governance can help agencies maximize the benefits of cloud technology while ensuring security, operational efficiency, and compliance:¹³

- Establish clear policies and procedures that outline the rules, standards, and guidelines for data security, access management, change management, incident response, and compliance. Clearly defined expectations ensure consistent and standardized practices across an agency's cloud environments.
- Define and assign clear roles and responsibilities to personnel responsible for managing and overseeing cloud resources, such as cloud administrators, security officers, compliance officers, and data stewards. Clearly defined roles ensure accountability and streamline decision-making processes, enabling efficient cloud governance.
- Establish and enforce robust security controls to protect cloud environments and data, such as implementing strong access management, encryption mechanisms, network segmentation, intrusion prevention and detection systems, and routine vulnerability assessments. Prioritizing security can mitigate risks and safeguard sensitive information.
- Continuously monitor and audit cloud resources to maintain compliance and identify potential security issues. Agencies should leverage monitoring tools and employ robust logging mechanisms to track activities within their cloud environments. Regular audits help identify gaps, address vulnerabilities, and ensure adherence to governance policies and regulatory requirements.
- Follow a well-defined change management process when making changes to cloud environments, to include evaluating the impact of changes, obtaining proper approvals, and conducting thorough testing before implementing changes. Effective change management practices help mitigate the risks associated with system disruptions and ensure smooth operations within the cloud environment.

¹³ IT Convergence [Cloud Governance Best Practices to Ensure Security & Compliance \(itconvergence.com\)](https://www.itconvergence.com).

- Provide regular training sessions and awareness programs to employees, emphasizing the importance of adhering to governance policies, recognizing potential security threats, and understanding their roles in ensuring cloud governance.
- Periodically review governance frameworks, policies, and procedures to ensure they remain effective and aligned with evolving business needs and regulatory requirements. By staying proactive and adaptable, organizations can optimize their cloud governance practices.



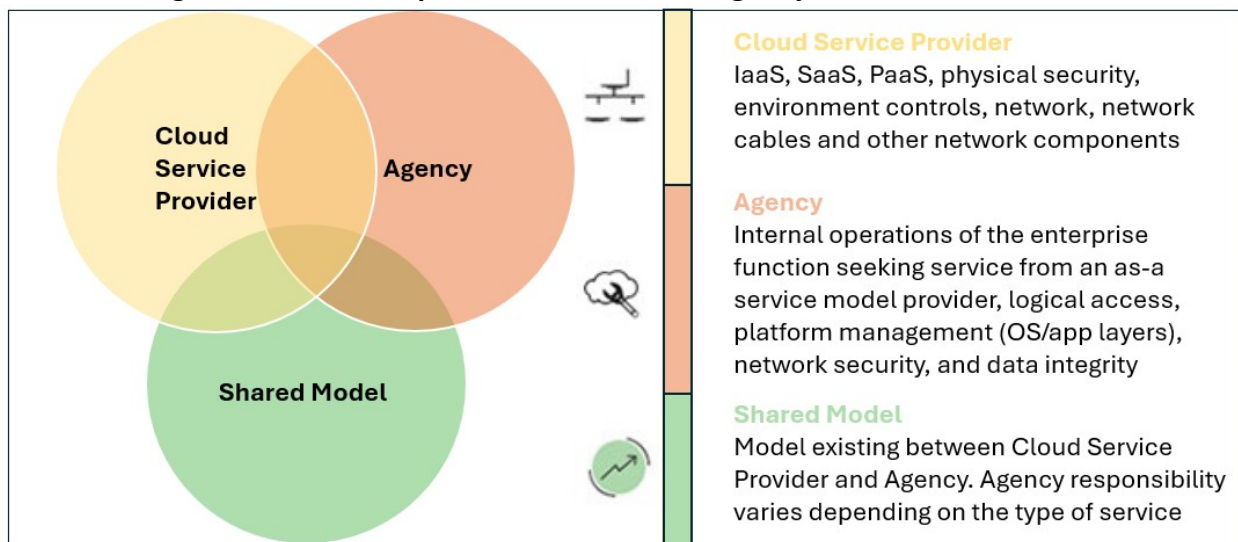
Risk

The adoption of cloud computing changes how an agency identifies, assesses, and treats risk. It is important for an agency to coordinate with the CSP to evaluate potential vulnerabilities and threats to the cloud infrastructure, applications, and data; and implement appropriate measures to mitigate, avoid, transfer, or accept each risk.

Best Practice 3: Reviewing service agreements ensures risk mitigation measures have been agreed upon.

Risk management for cloud services is based on the shared responsibilities model ([See Figure 2](#)), which lays out what the CSP and the agency is responsible for and depends on the type of services the agency wants to use. Normally, the CSP is responsible for managing the security of the actual cloud and associated infrastructure, which leaves the agency responsible for securing its own information and other assets stored in the cloud. Agencies should perform a risk assessment prior to implementing cloud services and document agreed upon risk mitigation measures in a service agreement. This provides a basis for reviewing the implementation of applicable security controls.

Figure 2: Shared Responsibilities Between Agency and Service Providers



Source: Information Systems Audit and Control Association (ISACA) [Understanding the Shared Responsibilities Model in Cloud Services](#).



Compliance

As with security, compliance in the cloud is also based on a shared responsibility model. Both the CSP and agency have responsibilities, but the agency is always responsible for ensuring its own compliance. These responsibilities are defined through contracts, audits, and assessments of the compliance requirements. Specifically, CSPs, agencies, and auditors must consider and understand the following:

- Regulatory implications for using a particular cloud service or CSP.
- Assignment of compliance responsibilities between the CSP and agency, including indirect providers (i.e., the CSP of your CSP).
- CSP capabilities for demonstrating compliance, including document generation, evidence production, and process compliance, in a timely manner.

Best Practice 4: Reviewing artifacts will ensure CSPs and agencies comply with security and performance expectations.

To ensure compliance, all contracts should include applicable information security clauses and both parties should understand what is expected in terms of evidence needed to demonstrate compliance. Contracts should also include service level agreements that define the level of performance expected from the CSP, how that performance will be measured, and what enforcement mechanisms will be used to ensure the specified levels are achieved.

While ensuring expectations are included in the contract and supporting documentation are covered in [Best Practice 1](#), both CSPs and agencies are also responsible for producing and managing their respective artifacts to support compliance with the established expectations. Examples of artifacts that may be reviewed include:

- *Third-Party Attestations* that certify compliance with regulations and industry standards.
- *A System Security Plan* that documents the security controls required for compliance.
- *A Control Implementation Summary* that documents the security responsibilities for both the agency and CSP.
- *A Security Assessment Report* that documents identified security deficiencies.

- A *Remedial Action Plan* that documents how the identified security deficiencies will be addressed with a planned date for completing the mitigation activities.
- *Performance Monitoring* data that documents compliance with service agreements, such as up-time, response times, timely resolution of problems, etc.
- *Audit logs* that record activities and events within a system.



Common Security Controls

Although many security and privacy controls are outsourced to the CSP, there are still many controls that the agency is responsible for. However, as discussed above, this depends on the cloud service model and the risk of the cloud service to the agency.

Once the agency understands their security-related responsibilities according to the shared responsibility model of their CSP, they must then determine the controls that are applicable in their use case.¹⁴ Agency responsibility varies based on many factors, including cloud services and the model they choose, the integration of those services into their IT environment, and the laws and regulations applicable to their organization and workload. The NIST Special Publication 800-53, Rev. 5, [Security and Privacy Controls for Information Systems and Organizations](#) (September 2020) provides a catalog of security and privacy controls for information systems and organizations. [Table 2](#) provides a summary of controls that are typically owned by either the agency or CSP based on the service model.

¹⁴ Use case is defined as a specific situation in which a product or service could potentially be used.

Table 2: Ownership of Security Controls based on Cloud Service Model

Control Area	IaaS	SaaS	PaaS
Physical Controls – Physical access to data centers is restricted to authorized personnel and mechanisms are in place to minimize the effect of a malfunction or physical disaster to data center facilities	CSP	CSP	CSP
Data integrity and confidentiality – Controls to provide reasonable assurance that data handling between the customer and the host service provider is secure	Agency	Agency	Agency
Identity and Access Management	Agency	Shared	Shared
Access policies – Logical access restriction to ascertain unauthorized access	Agency	Agency	Agency
Identity management – Secure control access to services and resources for users	Agency	CSP	CSP
Access and authentication – Multifactor authentication controls across layers of access to the environment	Agency	CSP	CSP
Application Layer Processes	Agency	Shared	CSP
Application security – Controls such as hardening or patch management used to ascertain adequate security	Agency	CSP	CSP
Application specific logic and code – Controls around the entire application development life cycle	Agency	Agency	CSP

Source: ISACA [Understanding the Shared Responsibilities Model in Cloud Services](#).

Given this, OIGs should consider the following best practices while conducting an audit of their agency’s cloud security. These best practices address the common controls that are typically the responsibility of the agency across all cloud service models and risk levels (i.e., access controls, data security, configuration management, continuous monitoring, and asset management).

Best Practice 5: Assessing roles and privileges will identify if roles are appropriately granted and in accordance with common security practices, such as the least privilege principle.

Access control is the process of granting or denying specific requests for obtaining and using information and related information processing services.¹⁵ Included is Identity and Access Management (IAM), which is deeply impacted by cloud computing. In cloud environments, both the CSP and the agency are required to manage IAM without compromising security. According

¹⁵ NIST SP 800-53, Rev. 5, [Security and Privacy Controls for Information Systems and Organizations](#) (September 2020).

to the Cloud Security Alliance,¹⁶ the CSP is typically responsible for enforcing authorizations and access controls while the agency is typically responsible for defining roles and properly configuring them within the cloud platform.¹⁷ Further, NIST has required security controls for agencies to implement and OIGs to consider while conducting an audit in this area, such as:

- 1) NIST SP 800-53, rev. 5 Control AC-3: Access Enforcement, states that organizations should enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
- 2) NIST SP 800-53, rev. 5 Control AC-6: Least Privilege, states that organizations should employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Best Practice 6: Assessing data requirements will identify what data is allowed to be stored in the cloud.

Data security is the process of maintaining the confidentiality, integrity, and availability of an agency's data in a manner consistent with the agency's risk strategy. Data security is also synonymous with information security, defined as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide integrity, confidentiality, and availability.¹⁸

Federal agencies will want some means of managing what data is stored by the CSP and should have defined policies for which data types are allowed or disallowed in the cloud environment. OIGs should consider if their agency has these baseline data requirements in place to ensure the agency can identify what data they store in the cloud environment. This may include data governance frameworks and having a comprehensive data inventory. Further, agencies should ensure data is protected as it is stored or moves between different platforms. NIST has a required security control for agencies to implement and OIGs to consider while conducting an audit in this area:

- 1) NIST SP 800-53, rev. 5 Control CM-12: Information Location, addresses the need to understand where information is being processed and stored. This includes identifying where specific information types and information reside in system components and how information is being processed so that information flow can be understood, and adequate protection and policy management can be provided for such information.

¹⁶ The Cloud Security Alliance is an organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment.

¹⁷ Cloud Security Alliance [Security Guidance for Critical Areas of Focus in Cloud Computing version 4.0](#) (July 2017).

¹⁸ OMB Circular A-130, [Managing Information as a Strategic Resource](#) (July 2016).

Best Practice 7: Assessing configuration settings will provide assurance that the system is configured according to the agency's operational requirements.

Configuration management is a collection of activities focused on establishing and maintaining the integrity of IT products and systems through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development lifecycle.¹⁹ This involves establishing a clear approach to documentation, maintenance, and change control so that systems can be configured consistently and accurately across cloud environments. Cloud platforms typically have baseline configurations or tools for agencies to implement; therefore, the responsibility still lies with the agency. These tools can help systems administrators keep track of the current state of applications and services to maximize performance and minimize security issues. NIST has a required security control for agencies to implement and OIGs to consider while conducting an audit in this area:

- 1) NIST SP 800-53, rev. 5 Control CM-6: Unsupported System Components, states that organizations should establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements; implement the configuration settings; identify, document, and approve any deviations from established configuration settings based on organization-defined operational requirements; and monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Best Practice 8: Ensuring audit logs are maintained and reviewed will provide visibility into identified vulnerabilities and threats.

Continuous monitoring is maintaining an ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.²⁰ Typically, cloud platform logs are provided by the platform itself. Agencies and CSPs should ensure that their monitoring scope sufficiently covers what is logged and where gaps are identified. In many cases, these can be automated system activities. The importance of continuous monitoring is being able to maintain visibility over the agencies' cloud environments and discover any vulnerabilities or threats to send alerts to agencies' security teams to remediate. NIST has a special publication for agencies to implement and OIGs to consider while conducting an audit in this area:

- 1) NIST SP 800-92, [Guide to Computer Security Log Management](#), states that routine log reviews and analysis are beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred, and for providing information useful for resolving such problems.

¹⁹ NIST SP 800-53, Rev. 5, [Security and Privacy Controls for Information Systems and Organizations](#) (September 2020).

²⁰ NIST SP 800-137, [Information Security Continuous Monitoring for Federal Information System](#) (September 2011).

Best Practice 9: Determining if the agency has complete and up-to-date information regarding their cloud inventory will ensure the agency does not have shadow IT.

IT asset management refers to the process or set of business practices used to track, manage, and organize the IT assets of the agency. Unmaintained assets or unneeded undisposed assets can pose risks to the agency as versions that are no longer used are more prone to outside security attacks or vulnerabilities. Similarly, running unneeded software incurs extra maintenance costs, which could otherwise be used for other IT systems or initiatives. Lastly, shadow IT is the use of hardware or software by an organization without the knowledge of the IT or security group within the organization. Shadow IT also poses security and cost concerns to the agency. NIST has required security controls for agencies to implement and OIGs to consider while conducting an audit in this area:

- 1) NIST SP 800-53 Rev 5, Control SI-2: Flaw Remediation, states that organizations should install security-relevant software and firmware updates. Organizations should have a policy regarding how many days updates need to be installed since the day of their release.
- 2) NIST SP 800-53 Rev 5, Control SA-22: Unsupported System Components, states that organizations should replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or provide these options for alternative sources for continued support for unsupported components, whether in-house or from external providers.



Appendix 1-Sample Audit Plan

This appendix provides sample procedures that can be used by an OIG while conducting a cloud security assessment for their agency. These procedures also align with the NIST criteria referenced above.

Common Control Group	Criteria	Objective	Audit Procedures
Governance, Risk, and Compliance	OMB, Federal Cloud Computing Strategy (Cloud Smart) (June 2019). Cloud Security Alliance Cloud Computing Matrix V4.0.4 (December 2021).	To ensure effective and sustainable management processes that result in transparency of business decisions, clear lines of responsibility, information security in alignment with regulatory and customer organization standards, and accountability.	<ol style="list-style-type: none">1) Determine if the IT, information security, and key business functions have defined integrated governance framework and monitoring processes.2) Determine if the IT, information security functions, and key business units are actively involved in the establishment of service level agreements and contractual obligations.3) Determine if the CSP has identified control objectives for provided cloud services.4) Determine that the agency cannot procure cloud services without the involvement of IT and information security personnel.5) Determine if the responsibilities for governance are documented and approved by the CSP and agency.6) Determine if roles and responsibilities are established and reporting relationships between the CSP and agency are clearly defined, identifying the responsibilities of both organizations.7) Determine whether the agency and CSP maintain documentation to support compliance with agreed upon contractual terms and service level agreements.
Access Controls	NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and	To determine if cloud system access privileges are consistent with security principles such as least	<ol style="list-style-type: none">1) Obtain a list of the roles within a system through Role-Based Access Control documents and determine if they are appropriate.2) Determine whether roles are appropriately assigned to employees in accordance with internal policies, including any circumvention of standard account provisioning process.

	<u>Organizations</u> (September 2020).	privilege and separation of duties.	<ol style="list-style-type: none"> 3) Determine the appropriateness of privileged roles and whether they were provisioned in accordance with least privilege and separation of duties. 4) Determine whether administrators can grant themselves additional access. 5) Determine if management has a process to terminate access after separation or an extended period of inactivity.
Data Security	<p>NIST SP 800-53, Rev. 5, <u>Security and Privacy Controls for Information Systems and Organizations</u> (September 2020).</p> <p>Federal Information Processing Standard (FIPS) 140-2, <u>Security Requirements for Cryptographic Modules</u> (May 2001).</p>	To determine whether cloud system data is properly encrypted in transit and at rest.	<ol style="list-style-type: none"> 1) Determine the data elements and connections that are encrypted in-transit and at-rest for the platform or application. 2) Determine whether the platform or application data is encrypted and complies with standard NIST criteria, FIPS 140-2, or internal agency guidance.
Configuration Management	NIST SP 800-53, Rev. 5, <u>Security and Privacy Controls for Information</u>	To determine the involvement of the agency in the change or control process.	<ol style="list-style-type: none"> 1) Obtain an understanding of the agency's change management process. 2) Determine whether change management processes are executed in accordance with agency policy.

	<p><u>Systems and Organizations</u> (September 2020).</p>		<ol style="list-style-type: none"> 3) For a sample change in the application, determine if it was appropriately migrated through the quality assurance and prototyping environments and included the approvals of the application owner and the cloud support team. 4) Using the applications or platforms and agency’s best practices, identify misconfigurations within the implementation or key settings. 5) Confirm any deviations from best practices are documented and the risks are accepted.
<p>Continuous Monitoring</p>	<p>NIST SP 800-53, Rev. 5, <u>Security and Privacy Controls for Information Systems and Organizations</u> (September 2020).</p> <p>NIST SP 800-92, <u>Guide to Computer Security Log Management</u> (September 2006).</p>	<p>To determine the ongoing effectiveness of controls.</p>	<ol style="list-style-type: none"> 1) Confirm whether the system has an active Authority to Operate in place through the FedRAMP process or internal agency guidelines. 2) Through inspection of control requirements, determine the security controls the agency is required to review on a periodic basis. 3) Confirm that the agency reviewed the required security controls via a Security Controls Assessment, documented the results, and created Plans of Actions and Milestones (POA&Ms) for any security controls that require remediation. 4) Inspect documentation that the agency has reviewed the CSP’s Security Controls Assessment and POA&Ms and documented accepted the risks of any weaknesses. 5) Identify the agency’s Security Information and Event Management (SIEM) tool. 6) Inquire specifically about whether use cases are developed for each platform and individual cloud applications. Determine the adequacy of the use cases for identifying suspicious activity on the cloud platforms. 7) Determine the nature of the event logs that are forwarded from the application or platform to the SIEM tool. 8) Determine whether application staff review audit logs in accordance with policy.

			9) For a sample event, determine whether follow-up actions were appropriately performed.
Asset Management	NIST SP 800-53, Rev. 5, <u>Security and Privacy Controls for Information Systems and Organizations</u> (September 2020).	To determine if there is a complete and accurate inventory of cloud applications and components.	<ol style="list-style-type: none"> 1) Obtain an understanding of the system inventory. 2) Confirm the number of applications supported by the cloud platform through inquiry. 3) Determine whether the data is accurately reflected on agency cloud inventories. 4) Confirm each platform and application is authorized through appropriate internal guidance. 5) Determine what products or subscriptions are used by the platform or application. 6) Inspect the systems documentation and service descriptions to determine that the data for products and subscriptions are accurately reflected. 7) Determine whether agency has any involvement with regards to the platform or application patching process. 8) If it is agency's responsibility, determine if platform or system releases, third-party applications, and custom release patches are evaluated internally by the systems administrators, tested, and deployed by the appropriate team during announced maintenance periods.



Appendix 2-Example OIG Reports

The working group reviewed and analyzed 19 federal oversight reports related to cloud governance and security. The table below identifies the control groups related to the findings of each report.

Report No.	Agency OIG	Audit Report	Cloud Governance	Access Control	Data Security	Configuration Management	Continuous Monitoring	Asset Management
DP-AR-13-004(R)	United States Postal Service	U.S. Postal Service Data Governance (April 23, 2013)	X					
IT-AR-14-009	United States Postal Service	Management of Cloud Computing Contracts and Environment (September 4, 2014)	X				X	X
19-016-R20	United States Postal Service	Business Application Review of the HERO System (August 24, 2020)	X				X	
IT-AR-15-009	United States Postal Service	Software Contract and Compliance Review (September 18, 2015)	X	X	X		X	
DOE-OIG-23-18	Department of Energy	Security over Cloud Computing Technologies at Select Department of Energy Locations (March 30, 2023)			X		X	X
DODIG-2023-052	Department of Defense	Audit of DoD's Compliance with Security Requirements When Using Commercial Cloud Services (February 15, 2023)					X	
DODIG-2020-079	Department of Defense	Report on the Joint Enterprise Defense Infrastructure (JEDI) Cloud	X					

Report No.	Agency OIG	Audit Report	Cloud Governance	Access Control	Data Security	Configuration Management	Continuous Monitoring	Asset Management
		Procurement (April 13, 2020)						
2023-20-018	Treasury Inspector General for Tax Administration	The Enterprise Case Management System Did Not Consistently Meet Cloud Security Requirements (March 27, 2023)	X					
OIG-19-015-A	Department of Commerce	The Census Bureau Must Correct Fundamental Cloud Security Deficiencies in Order to Better Safeguard the 2020 Decennial Census (June 19, 2019)	X			X		
A-14-18-50498	Social Security Administration	Security of the Social Security Administration's Cloud Environment (March 23, 2022)				X		
22-02961-71	Department of Veteran Affairs	Inspection of Information Security at the St. Cloud VA Medical Center in Minnesota (June 8, 2023)	X	X		X		
IG-17-010	National Aeronautics and Space Administration	Security of NASA's Cloud Computing Services (February 7, 2017)				X		
OIG-AR-15-05	Export-Import Bank	Independent Audit of the EXIM's Planning and Implementation of FMS-NG (March 31, 2015)	X	X				

Report No.	Agency OIG	Audit Report	Cloud Governance	Access Control	Data Security	Configuration Management	Continuous Monitoring	Asset Management
A-000-15-006-P	U.S Agency for International Development	Audit of USAID's Progress in Adopting Cloud Computing Technologies (March 12, 2025)	X		X			X
DODIG-2023-052	Department of Defense	Audit of the DoD's Compliance with Security Requirements When Using Commercial Cloud Services (February 15, 2023)					X	
A-18-17-09304	Health and Human Services	The National Institutes of Health Could Improve Its Monitoring to Ensure That an Awardee of the All of Us Research Program Had Adequate Cybersecurity Controls to Protect Participants' Sensitive Data (June 10, 2019)	X		X		X	
556	Securities and Exchange Commission	The SEC Can More Strategically and Securely Plan, Manage, and Implement Cloud Computing Services (November 7, 2019)	X		X			
AUD-2023-002	Federal Housing Finance Agency	FHFA Did Not Fully Implement Select Security Controls Over One of Its Cloud Systems as Required by NIST and FHFA Standards and	X			X		

Report No.	Agency OIG	Audit Report	Cloud Governance	Access Control	Data Security	Configuration Management	Continuous Monitoring	Asset Management
		Guidelines (March 8, 2023)						
IG-15-01-SR	Peace Corps	Management Advisory Report: The Peace Corps' Cloud Computing Pilot Program (March 17, 2015)	X	X	X	X	X	



Appendix 3-Key Terms and Definitions

Access Control	The process of granting or denying specific requests for obtaining and using information and related information processing services.
Asset Management	The process or set of business practices used to track, manage, and organize the IT assets of the organizations.
Authority to Operate	An official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
Cloud Computing	A model for enabling ubiquitous, 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.
Cloud Service Model	<p>There are many options when moving infrastructure, applications, or services into the cloud. NIST has defined three basic cloud service models: SaaS; PaaS; and IaaS.</p> <ul style="list-style-type: none">• SaaS: Consumers are users of the provider’s applications running on an underlying cloud infrastructure. Applications are accessible via various client platforms. Consumers do not manage or control the underlying infrastructure.• PaaS: Consumers have the capability to deploy custom applications using provider-supplied languages, libraries, services, and tools on the cloud infrastructure. Consumers do not manage or control the underlying infrastructure, but they have control over the deployed applications and potentially the configuration settings of the provider-supplied environment that is hosting the application.• IaaS: Consumers have the capability to provision computing resources to deploy and run environments and applications. Cloud providers manage the underlying infrastructure while the consumers have control over the computing resources, including some control of selected networking components (e.g., host- versus network-based firewall).
Cloud Service Provider (CSP)	An external company that provides a platform, infrastructure, applications, and/or storage services for its clients.

Configuration Management	A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development lifecycle.
Continuous Monitoring	Continuous monitoring is defined as maintaining an ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
Data Security	The process of maintaining the confidentiality, integrity, and availability of an agency's data in a manner consistent with the agency's risk strategy.
Federal Risk and Authorization Management Program (FedRAMP)	FedRAMP is a governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
Service Level Agreement	A service contract that defines the specific responsibilities of the service provider and sets the customer's expectations.
Shared Responsibility Model	A model that outlines the different responsibilities between the customer and the CSP.



List of Contributors

This report was developed under the guidance of the FAEC Cross-cutting Issues Subcommittee chaired by leadership from Export-Import Bank of the United States OIG and Environmental Protection Agency OIG. Special thanks to the FAEC Cross-cutting Issues Subcommittee working group members who contributed their time and expertise to this effort from the following OIGs:

U.S. Postal Service OIG

Federal Deposit Insurance Corporation OIG

U.S. Agency for International Development OIG