Office of Privacy,
Governmental Liaison & Disclosure

IRS Safeguards

Federation of Tax Administrators

Steve Matteson
steven.m.matteson@irs.gov
Corey Sinay
corey.sinay@irs.gov

Kansas City, MO
August 6, 2018

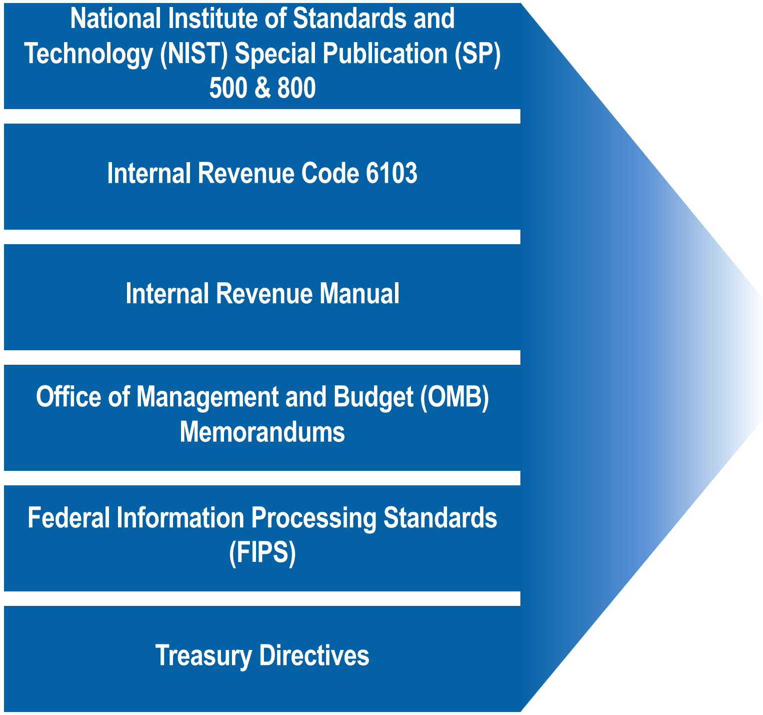
Agenda

- IRS Publication 1075 and Safeguards Assessment Methodology
- Updated Guidance from NIST and Anticipated Timeline for NIST SP 800-53 Rev. 5
- Safeguards Requirements for Cloud Providers
- Frequently Asked Questions

PUBLICATION 1075

IRS Publication 1075

- Publication 1075 provides information security requirements to agencies that receive, process, store or transmit federal tax information (FTI) under the provisions of Internal Revenue Code Section 6103.



National Institute of Standards and Technology (NIST) Special Publication (SP) 500 & 800

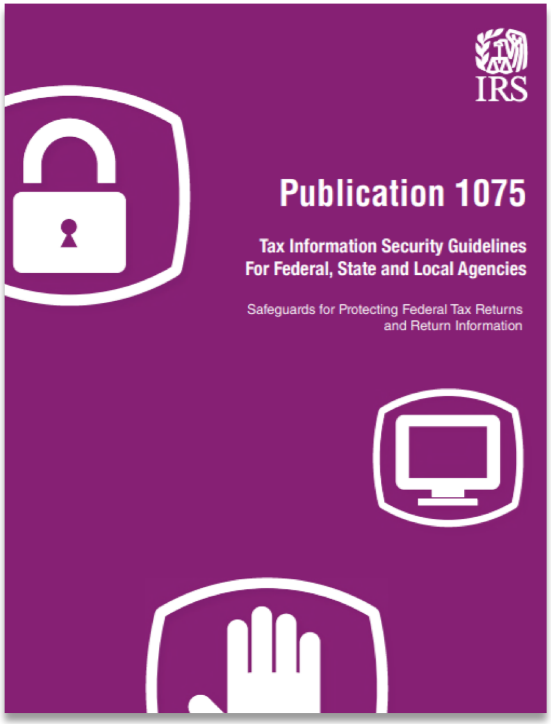
Internal Revenue Code 6103

Internal Revenue Manual

Office of Management and Budget (OMB) Memorandums

Federal Information Processing Standards (FIPS)

Treasury Directives



IRS

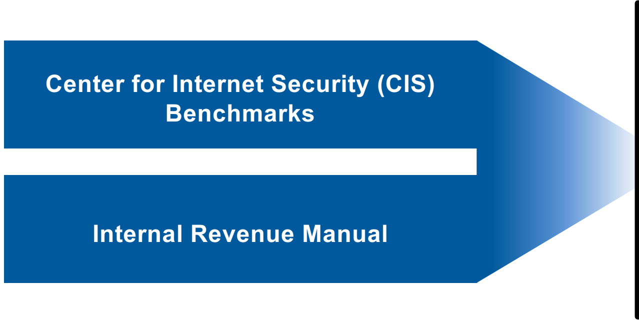
Publication 1075

Tax Information Security Guidelines
For Federal, State and Local Agencies

Safeguards for Protecting Federal Tax Returns
and Return Information

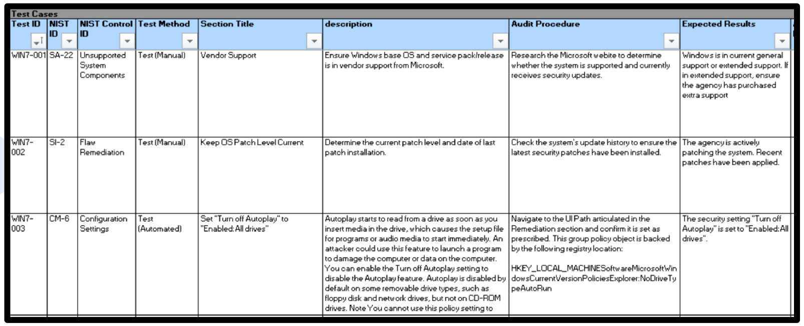
Safeguards Assessment Methodology

- Safeguards Computer Security Evaluation Matrices (SCSEMs) and Audit Profiles are informed by Publication 1075 requirements and controls, IRC 6103, and compliance requirements from the Center for Internet Security (CIS) Benchmarks
- Nessus is used to conduct configuration compliance checks using CIS benchmarks supplemented with IRS-specific requirements from Publication 1075 and IRC 6103.
- This process has been developed to provide agencies with enhanced information regarding the security controls in place to protect FTI.



Center for Internet Security (CIS) Benchmarks

Internal Revenue Manual



Test Cases

Test ID	NIST ID	NIST Control ID	Test Method	Section Title	description	Audit Procedure	Expected Results
WIN7-001	SA-22	Unsupported System Components	Test (Manual)	Vendor Support	Ensure Windows base OS and service pack/release is in vendor support from Microsoft.	Research the Microsoft webite to determine whether the system is supported and currently receives security updates.	Windows is in current general support or extended support. If in extended support, ensure the agency has purchased extra support
WIN7-002	SI-2	Flaw Remediation	Test (Manual)	Keep OS Patch Level Current	Determine the current patch level and date of last patch installation.	Check the system's update history to ensure the latest security patches have been installed.	The agency is actively patching the system. Recent patches have been applied.
WIN7-003	CM-6	Configuration Settings	Test (Automated)	Set "Turn off Autoplay" to "Enabled: All drives"	Autoplay starts to read from a drive as soon as you insert media in the drive, which causes the setup file for programs or audio media to start immediately. An attacker could use this feature to launch a program to damage the computer or data on the computer. You can enable the Turn off Autoplay setting to disable the Autoplay feature. Autoplay is disabled by default on some removable drive types, such as floppy disk and network drives, but not on CD-ROM drives. Note You cannot use this policy setting to	Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy object is backed by the following registry location: HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionPoliciesExplorer:NoDriveTypeAutoRun	The security setting "Turn off Autoplay" is set to "Enabled: All drives".

Microsoft Windows 7 SCSEM

CIS was selected as the benchmark organization for Safeguards because it most closely aligned with the computing environment needed for civil government agencies.

Safeguards Assessment Methodology (Cont.)

- An audit profile is created by beginning with the default CIS benchmark that is published for a particular technology and editing it to meet required IRS values.
- Safeguards creates an automated profile that will be used with Nessus to scan technologies during an onsite review based on CIS published benchmarks.
- If an automated profile is not available or the technology cannot be scanned, Safeguards conducts manual assessments.
- All assessments have some level of manual test cases.

Automated & Manual Checks

- Oracle 11g
- Oracle 12c
- SQL Server
- DB2 for Linux, Unix, & Windows
- MacOS
- Cisco ASA
- Cisco OS
- Unix/Linux
- AIX
- CentOS Linux
- HP-UX 11i
- Oracle Linux
- Oracle Solaris
- Red Hat Linux
- SUSE Linux Enterprise Server 11, 12
- ESXi
- Apache Linux
- Windows 10
- Windows 8-8.1
- Windows 7
- Windows Server 2008R2
- Windows Server 2008SP2
- Windows Server 2012
- Windows Server 2012R2
- Windows Server 2016

Manual Checks Only

- General Application
- Oracle Enterprise Taxation and Policy Management (ETPM)
- Fast Enterprises GenTax 8
- RSI Revenue Premier
- Teradata
- Data Warehouse
- DB2 for IBM z/OS
- DB for Generic
- Mainframe
- MOT
- Network Firewall, Assessment, SAN, SR, VoIP, VPN, Wireless Networking
- Cloud Computing
- Mobile Device
- OpenVMS
- Printer
- Generic VDI
- Generic Web

NIST Cloud Computing Reference Architecture – SP 500-292

"The NIST cloud computing reference architecture focuses on the requirements of "what" cloud services provide, not a "how to" design solution and implementation. The reference architecture is intended to facilitate the understanding of the operational intricacies in cloud computing." (NIST 500-292)

- Responsibilities of cloud provider versus tenant
  - Where do responsibilities fall for the CIA Triad?
    - Authentication
    - Logical Security (Firewall, Boundary)
    - Operational (Provisioning resources, operating system, hypervisors)

Security Control Implementation

Control Families from NIST SP 800-53 Rev. 4

- AC – Access Control
- AU – Audit and Accountability
- AT – Awareness and Training
- CM – Configuration Management
- CP – Contingency Planning
- IA – Identification and Authentication
- IR – Incident Response
- MA – Maintenance
- MP – Media Protection
- PS – Personnel Security
- PE – Physical and Environmental Protection
- PL – Planning
- PM – Program Management
- RA – Risk Assessment
- CA – Security Assessment and Authorization
- SC – System and Communications Protection
- SI – System and Information Integrity
- SA – System and Services Acquisition

MINIMUM Security Controls

- High-Impact Baseline
- Moderate-Impact Baseline
- Low-Impact Baseline

NIST controls for MODERATE are selected for Publication 1075

a) Control Enhancements are evaluated when putting together Publication 1075 requirements.

b) There is a focus on controls that enhance the confidentiality of data and controls that are meant for integrity or availability are less likely to be selected for Publication 1075. The team evaluates each control to see if it is applicable to Safeguards purview.

c) IRS defines the organization-defined parameters for the NIST controls.

Security Control Implementation – IA-5 Authenticator Management

NIST SP 800-53 IA-5 Authenticator Management Control Description

The organization manages information system authenticators by:

a. V
ide
aut
b. E
by
c. E
me
d. E
init
aut
e. C
sys
f. E
reu
g. C
def
h. F
mo
i. R
spe
j. C
membership to those accounts changes.

Control Enhancements: AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION

The information system, for password-based authentication:

(a) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];
(b) Enforces at least [Assignment: organization-defined number of changed characters] when new passwords are created;
(c) Stores and transmits only encrypted representations of passwords;
(d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization defined numbers for lifetime minimum, lifetime maximum]; and
(e) Prohibits password reuse for [Assignment: organization-defined number] generations.

Supplemental Guidance: This control enhancement applies to single factor authentication of individuals using passwords and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement typically does not apply when passwords are used to unlock hardware authenticators. The implementation of such password mechanisms may not meet all of the requirements in the enhancement. Encrypted representations of passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords.

IRS Publication 1075 Section 9.3.7.5 Authenticator Management (IA-5)

The agency must manage information system authenticators by:

a) The information system must, for password-based authentication: Enforce minimum password complexity of:
   1. Eight characters
   2. At least one numeric and at least one special character
   3. A mixture of at least one uppercase and at least one lowercase letter
   4. Storing and transmitting only encrypted representations of passwords
b) Enforce password minimum lifetime restriction of one day
c) Enforce non-privileged account passwords to be changed at least every 90 days
d) Enforce privileged account passwords to be changed at least every 60 days
e) Prohibit password reuse for 24 generations
f) Allow the use of a temporary password for system logon requiring an immediate change to a permanent password
g) Password-protect system initialization (boot) settings

membership to those accounts changes

Extracted from IRM

Security Control Testing: Nessus

- Agencies should prepare their systems and personnel to avoid any scanning issues during the on-site review. ***Nessus scanning at data centers should be prepped and ready to scan endpoints on Tuesday, as resources and schedules permit.***
- This checklist should serve as a tool to help prepare agencies for on-site automated Nessus testing:

    1. **Identify Personnel to support the review:**
        - Scan technicians, network technicians, system administrators, database administrators, and desktop services personnel are required to support Nessus activities
    2. **Create scope inventory document**
        - OS version, hostname, IP address
    3. **Define network location for scanning, whitelist scan engine**
        - Connectivity to target systems
    4. **Create credentials**
        - Admin (or root) username/password at domain and/or local level
        - Include credential in security groups (Unix)
    5. **Prepare systems - examples include:**
        - Disable UAC, enable remote registry and WMIC, open ports, test credentials
        - Disable lockdown mode
        - Enable SSH

- When performing test scans prior to an onsite visit, ensure scans are successful by validating the existence of “Compliance Details” for each host. Compliance details must be gathered in order for Safeguards to complete the assessment.
- Registry keys and other configuration elements need to be explicitly set and configured to meet Safeguards requirements. Using defaults or unconfigured items will lead to Nessus determining a NULL result which cannot be accepted.

NIST SP 800-53 REV. 5

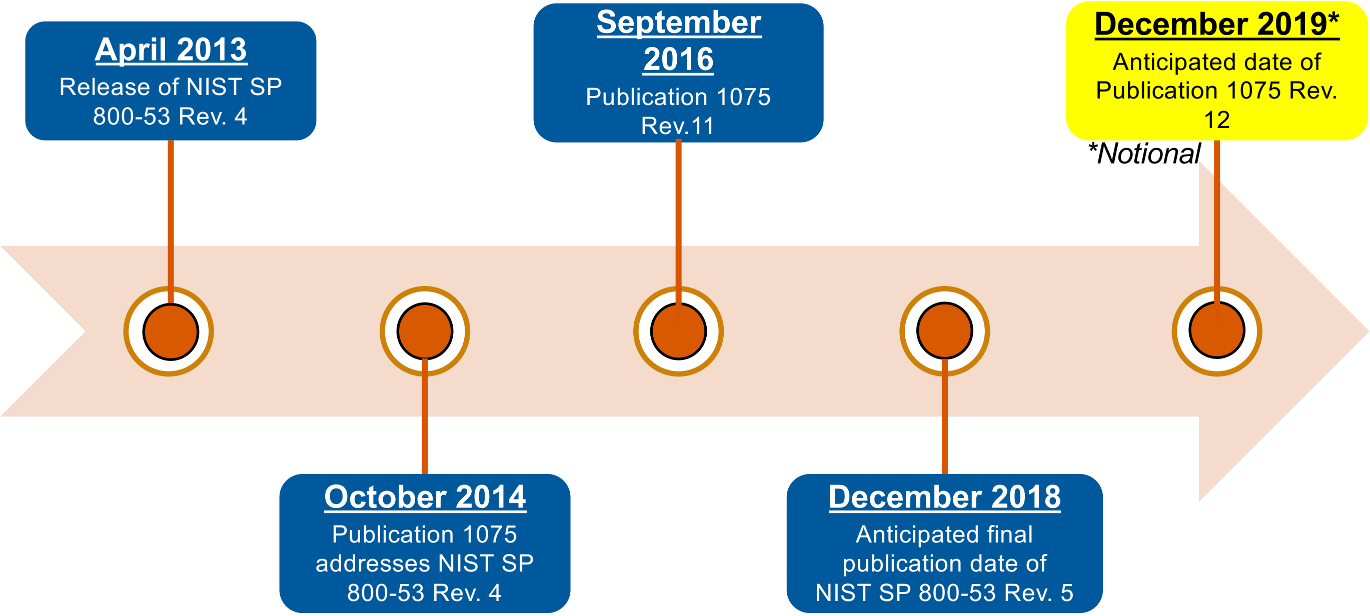
Updated Guidance from NIST

NIST SP 800-53 Rev. 5

- Scheduled for publication in the later half of 2018
- According to NIST, the major changes to the publication include:
  - Making the security and privacy controls more outcome-based by changing the structure of the controls
  - Fully integrating the privacy controls into the security control catalog creating a consolidated and unified set of controls for information systems and organizations, while providing summary and mapping tables for privacy-related controls
  - Separating the control selection process from the actual controls, thus allowing the controls to be used by different communities of interest including systems engineers, software developers, enterprise architects; and mission/business owners
  - Promoting integration with different risk management and cybersecurity approaches and lexicons, including the Cybersecurity Framework
  - Clarifying the relationship between security and privacy to improve the selection of controls necessary to address the full scope of security and privacy risks
  - Incorporating new, state-of-the-practice controls based on threat intelligence and empirical attack data, including controls to strengthen cybersecurity and privacy governance and accountability

NIST SP 800-53 Rev. 5 Anticipated Timeline

- NIST updates have historically been followed by a revised release of Publication 1075. IRS Office of Safeguards does not immediately test against new NIST guidelines until Publication 1075 is updated.



April 2013
Release of NIST SP 800-53 Rev. 4

October 2014
Publication 1075 addresses NIST SP 800-53 Rev. 4

September 2016
Publication 1075 Rev.11

December 2018
Anticipated final publication date of NIST SP 800-53 Rev. 5

December 2019*
Anticipated date of Publication 1075 Rev. 12

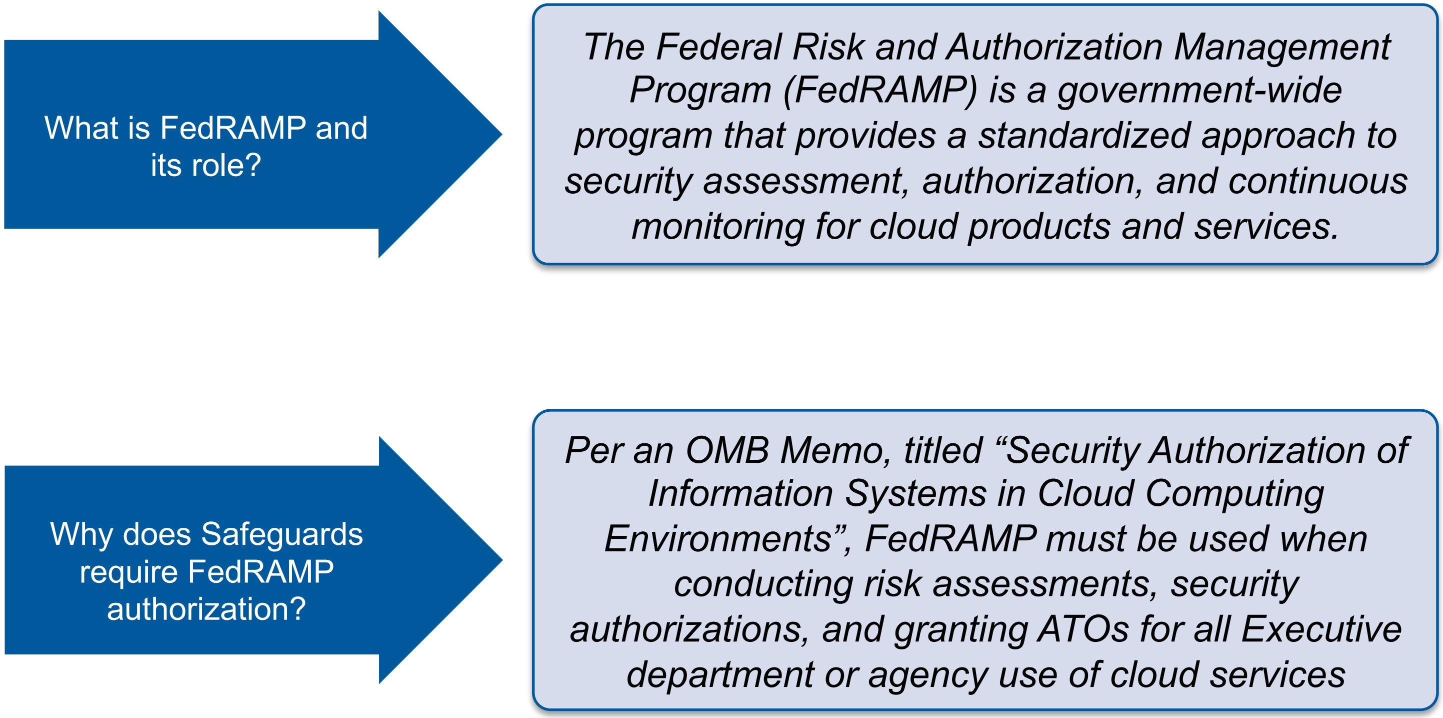
**Notional*

Impact of NIST SP 800-53 Rev. 5 on Federal and State agencies

- Updates to Publication 1075
- Updates to reporting requirements (SSR, 45-Day Notification, etc.)
- Updates to SCSEMs

CLOUD COMPUTING

FedRAMP Authorization



What is FedRAMP and its role?

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Why does Safeguards require FedRAMP authorization?

Per an OMB Memo, titled “Security Authorization of Information Systems in Cloud Computing Environments”, FedRAMP must be used when conducting risk assessments, security authorizations, and granting ATOs for all Executive department or agency use of cloud services

What is a Cloud?

NIST SP 800-145 defines a cloud as:

- 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.

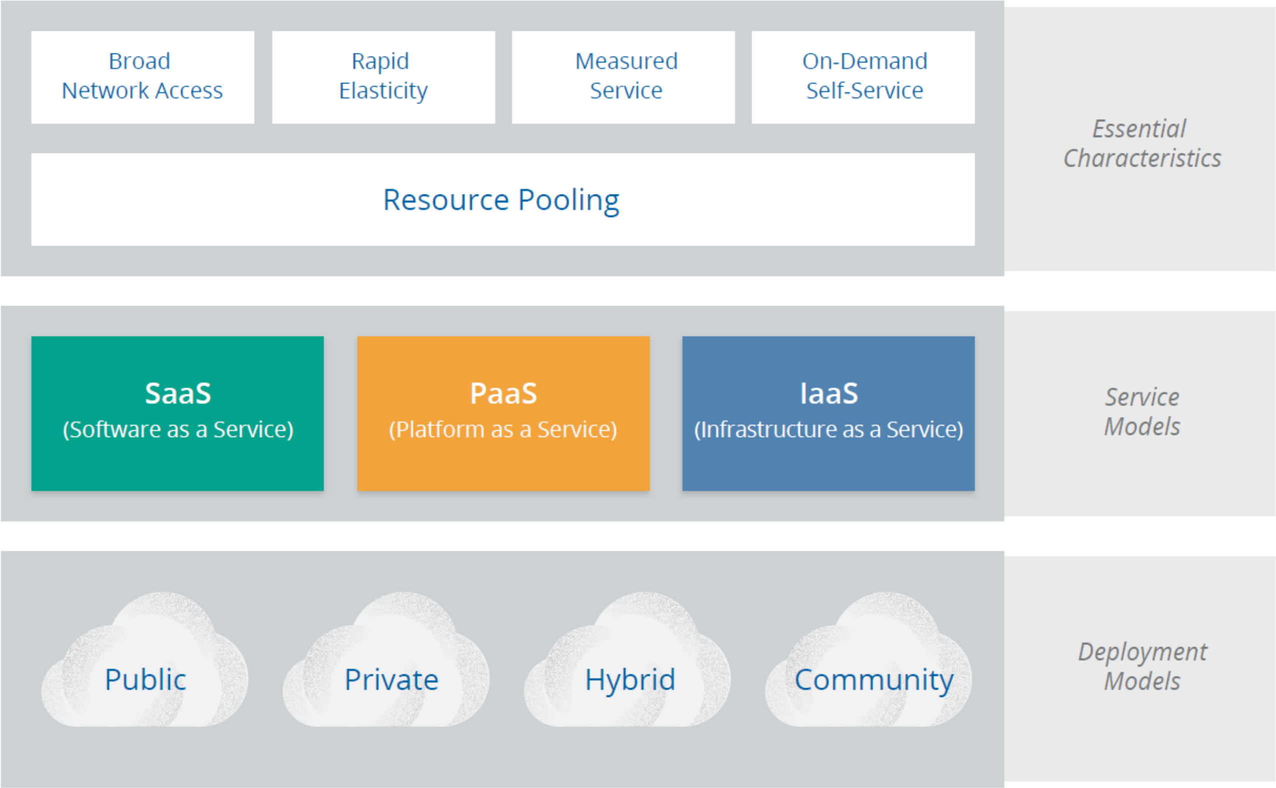
Determining a Cloud within the context of Safeguards

- Due to the nature of relationships between IRS, partner agencies, consolidated data centers and third parties, there may be some gray areas when determining whether FTI resides in a cloud environment *(non-exhaustive list of examples below)*
- Clouds processing FTI are subject to additional requirements (e.g. 45-Day Notification and use of Cloud SCSEM on review)

Safeguards Cloud	Not Safeguards Cloud
• **Traditional Cloud Services:** Instances where an agency has contracted with well-known cloud vendors for supporting/implementing FTI systems • **Data Storage Solutions**: Instances where an agency uses 3rd-party provided data storage and movement systems which meet cloud definition (multi-tenant, multiple facilities, etc.).	• **Contracted 3rd Party Services** (e.g., collections agencies) • **Hosted Solutions/Systems:** Agency maintains ownership and configuration of technologies located in a 3rd-party managed facility • **Contractor-Managed Consolidated Data Centers:** State has outsourced management of data center to contractor • **Agency-Managed Virtual Environments:** Agency has provisioned a virtual environment which hosts FTI systems

Cloud Basics

Essential Characteristics, Service Models, and Deployment Models for Cloud Computing.



Broad Network Access

Rapid Elasticity

Measured Service

On-Demand Self-Service

Resource Pooling

Essential Characteristics

SaaS (Software as a Service)

PaaS (Platform as a Service)

IaaS (Infrastructure as a Service)

Service Models

Public

Private

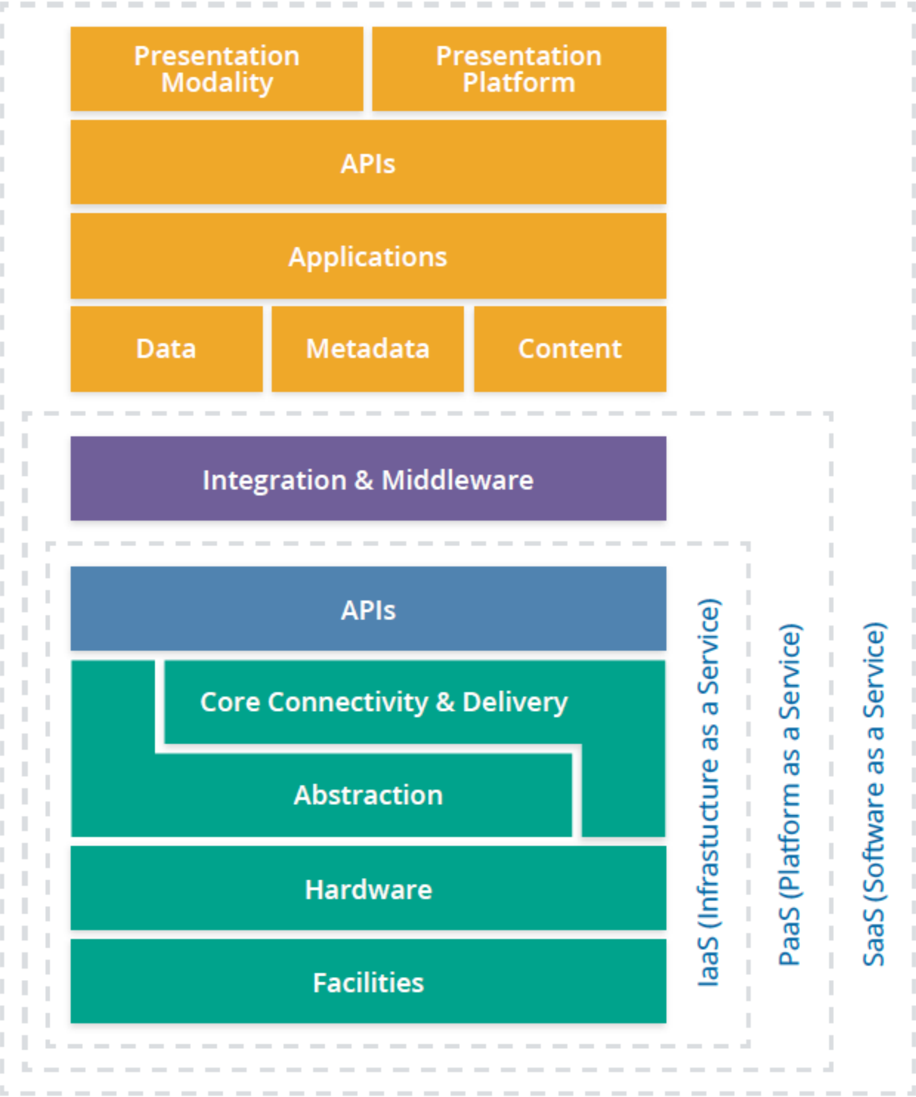
Hybrid

Community

Deployment Models

Source: Cloud Security Alliance: Security Guidance v4

Cloud Service Models

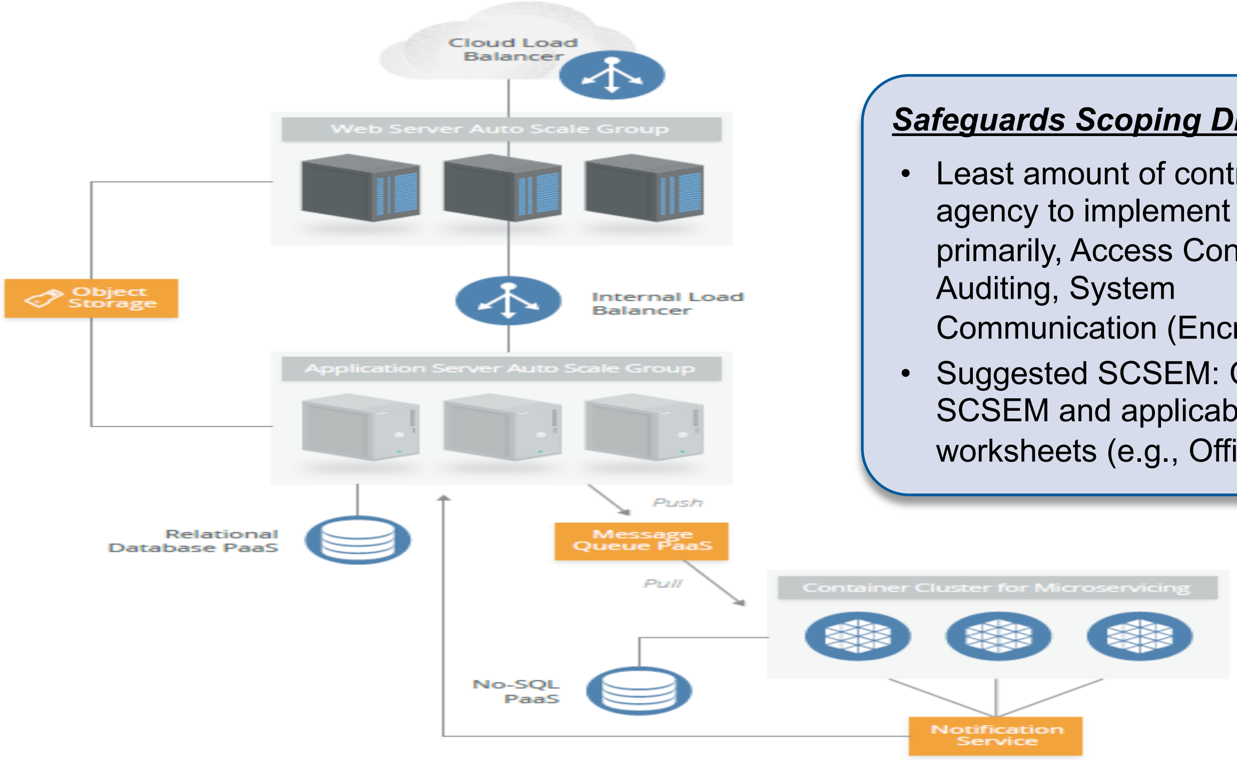


Source: Cloud Security Alliance: Security Guidance v4

Scoping Service Models: Software as a Service (SaaS)

A SaaS uses the provider's applications running on the provider's cloud infrastructure.

- Provider is responsible for the highest amount of security and data protection under this model
- Customer will negotiate into the service contract with the provider



Safeguards Scoping Discussion:

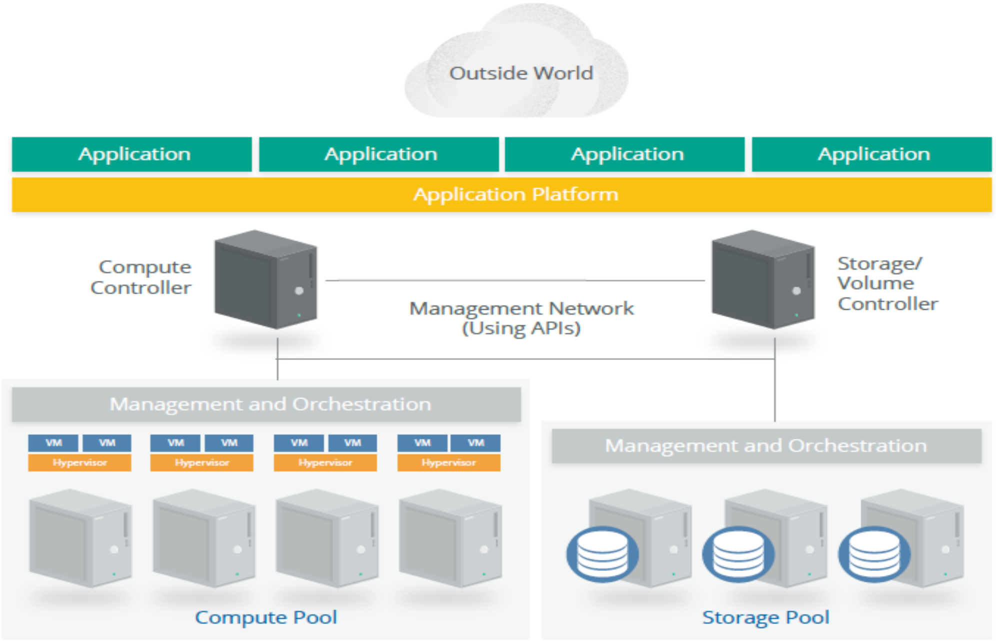
- Least amount of controls for agency to implement and test: primarily, Access Control, Auditing, System Communication (Encryption)
- Suggested SCSEM: Cloud SCSEM and applicable worksheets (e.g., Office 365)

Source: Cloud Security Alliance: Security Guidance v4

Scoping Service Models: Platform as a Service (PaaS)

Deploying customer-created or acquired applications created using programming languages and tools supported by the provider.

- Security is a shared responsibility with the provider responsible for the underlying platform infrastructure
- Customer is responsible for securing the applications developed and hosted on the platform



Source: Cloud Security Alliance: Security Guidance v4

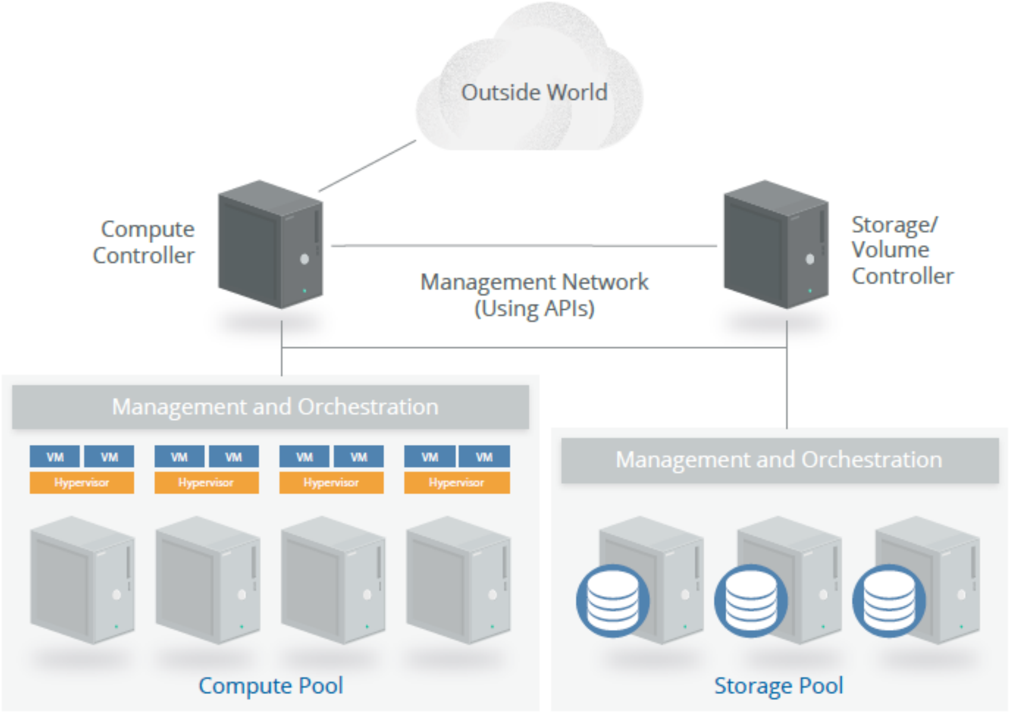
Safeguards Scoping Discussion:

- Moderate amount of controls for agency to implement and test: App development change management, database architecture, in addition to AC, AU, SC
- Suggested SCSEM: Cloud SCSEM, Application SCSEM, Database SCSEM

Scoping Service Models: Infrastructure as a Service (IaaS)

Provision processing, storage, networks, and other fundamental computing resources.

- Customer is responsible for the highest amount of security


Outside World
Compute Controller
Management Network (Using APIs)
Storage/ Volume Controller
Management and Orchestration
VM
Hypervisor
Compute Pool
Management and Orchestration
Storage Pool

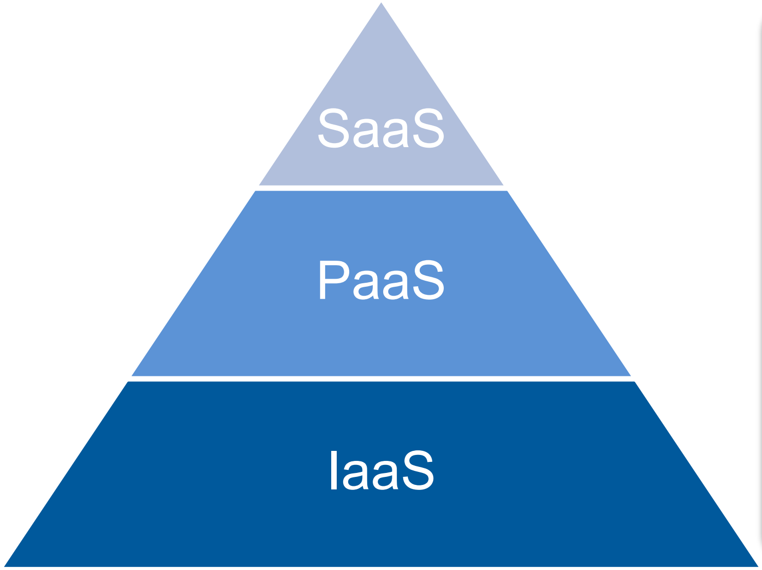
Source: Cloud Security Alliance: Security Guidance v4

<u>Safeguards Scoping Discussion</u>:

- Agency has the most controls to implement and test in this model. Agencies may be responsible for implementing configurations of: OS, DBMS, and web server technical configurations
- Suggested SCSEM: OS, DBMS, Application, Web Server, Boundary Protection (i.e., Firewall/VPN)

Protecting FTI in a Cloud Computing Environment

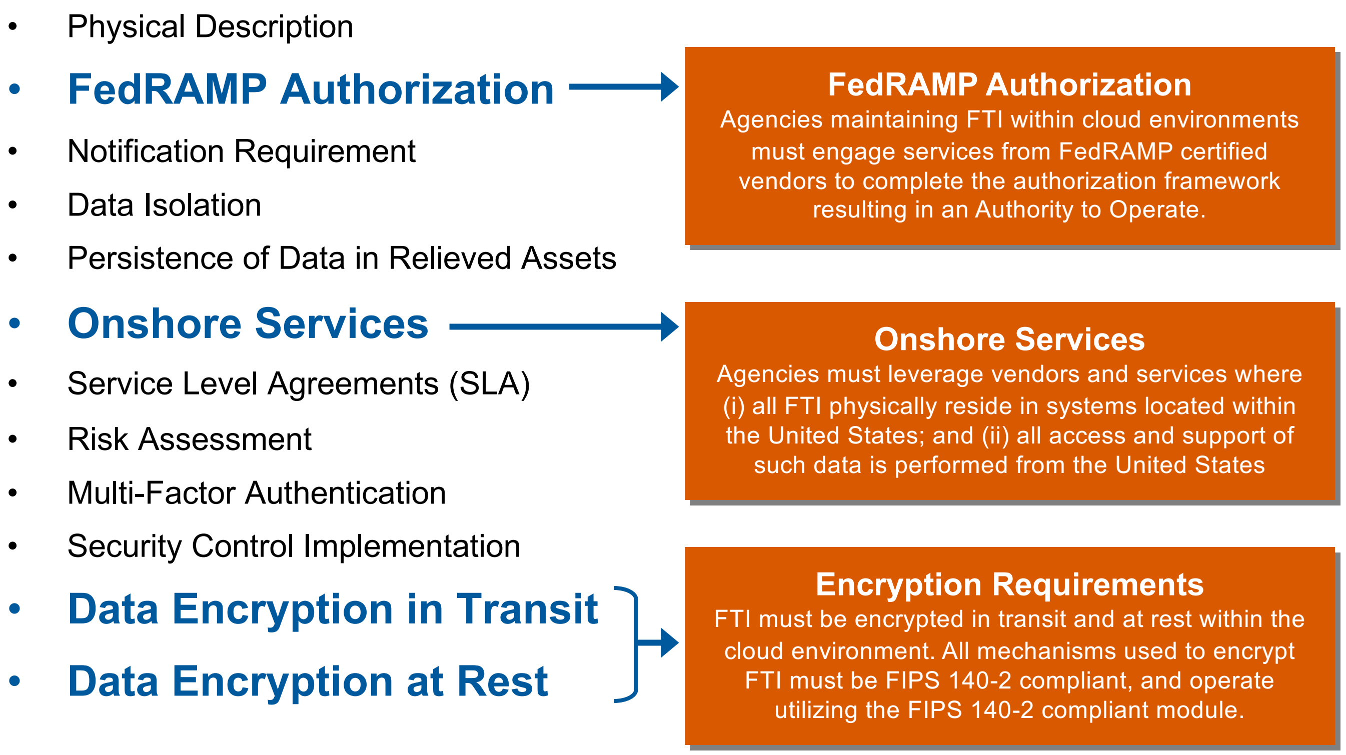
- As agencies look to reduce costs and improve operations, cloud computing may offer promise as an alternative to traditional data center models. By utilizing SaaS, PaaS, or IaaS cloud service models, agencies may be able to reduce hardware and personnel costs by eliminating redundant operations and consolidating resources.



While cloud computing offers many potential benefits, it is not without risk. Limiting access to authorized individuals becomes a much greater challenge with the increased availability of data in the cloud, and agencies may have greater difficulties isolating federal tax information (FTI) from other information and preventing "commingling" of data.

Cloud Providers: Cloud Requirements

- To use a cloud computing model to receive, transmit, store, or process FTI, the agency must be in compliance with all Publication 1075 requirements. The following mandatory requirements are in effect for introducing FTI to a cloud environment:



- Physical Description
- **FedRAMP Authorization**
- Notification Requirement
- Data Isolation
- Persistence of Data in Relieved Assets
- **Onshore Services**
- Service Level Agreements (SLA)
- Risk Assessment
- Multi-Factor Authentication
- Security Control Implementation
- **Data Encryption in Transit**
- **Data Encryption at Rest**

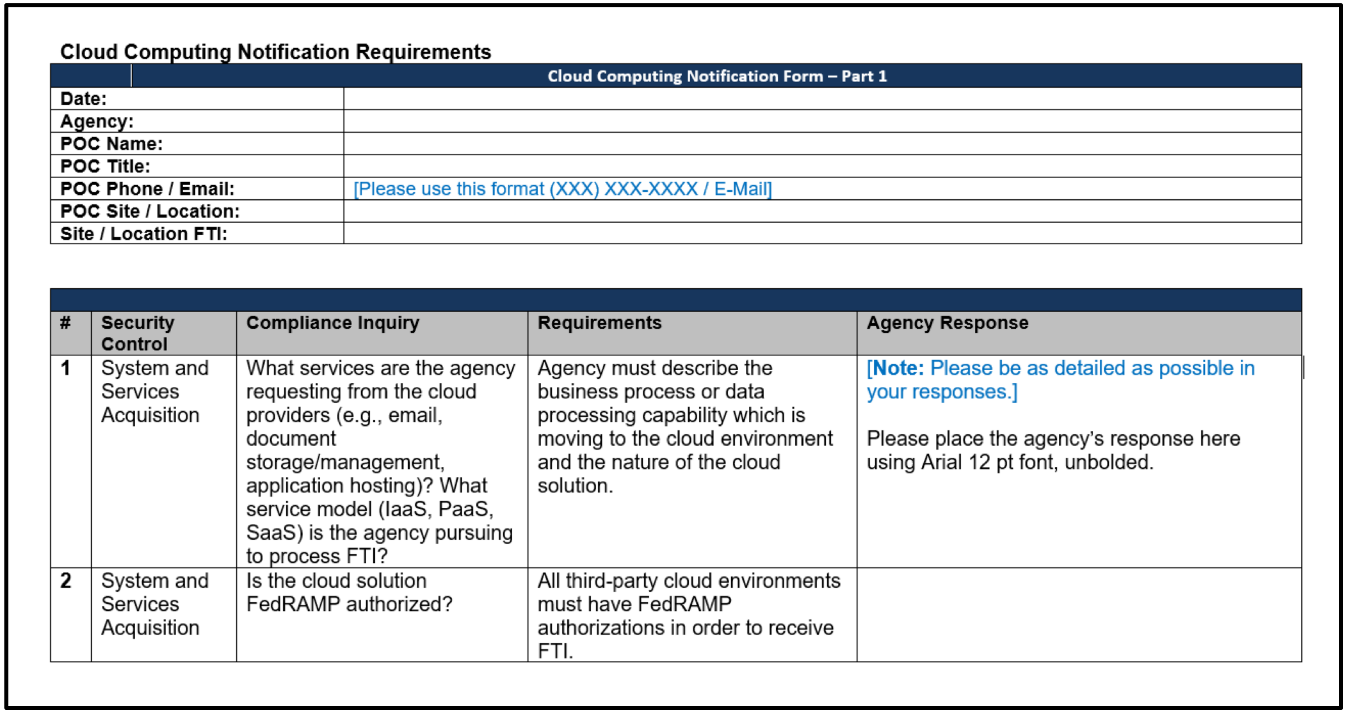
FedRAMP Authorization
Agencies maintaining FTI within cloud environments must engage services from FedRAMP certified vendors to complete the authorization framework resulting in an Authority to Operate.

Onshore Services
Agencies must leverage vendors and services where (i) all FTI physically reside in systems located within the United States; and (ii) all access and support of such data is performed from the United States

Encryption Requirements
FTI must be encrypted in transit and at rest within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant, and operate utilizing the FIPS 140-2 compliant module.

45-Day Notification for Cloud Computing

- To use a cloud computing model that receives processes, stores, or transmits FTI, the agency must notify the Office of Safeguards at least 45 days prior to transmitting FTI into a cloud environment.
- The Cloud Computing Notification form can be found on the IRS Office of Safeguards website: https://www.irs.gov/privacy-disclosure/additional-requirements-for-publication-1075



Cloud Computing Notification Requirements

Cloud Computing Notification Form – Part 1	
Date:	
Agency:	
POC Name:	
POC Title:	
POC Phone / Email:	[Please use this format (XXX) XXX-XXXX / E-Mail]
POC Site / Location:	
Site / Location FTI:	

#	Security Control	Compliance Inquiry	Requirements	Agency Response
1	System and Services Acquisition	What services are the agency requesting from the cloud providers (e.g., email, document storage/management, application hosting)? What service model (IaaS, PaaS, SaaS) is the agency pursuing to process FTI?	Agency must describe the business process or data processing capability which is moving to the cloud environment and the nature of the cloud solution.	[**Note:** Please be as detailed as possible in your responses.] Please place the agency's response here using Arial 12 pt font, unbolded.
2	System and Services Acquisition	Is the cloud solution FedRAMP authorized?	All third-party cloud environments must have FedRAMP authorizations in order to receive FTI.	

Cloud Security Considerations

- FedRAMP Authorization
  - Has the cloud solution received FedRAMP certification?
    - Must be at least FedRAMP Moderate, and must have a Provisional ATO (P-ATO) from the FedRAMP Joint Authorization Board (JAB)
- Physical Location
  - At which address will the cloud systems reside?
    - Must be physical address and must be located within the US
- Data Isolation
  - Who manages access control for data in the cloud?
    - FTI cannot be shared with other cloud tenants
    - FTI must only be disclosed to other organizations per IRC 6103(p)(4)
    - Account access must follow Need to Know and Least Privilege best practices

Cloud Security Considerations (Cont.)

- Remote Access
  - Can users access cloud environment outside agency network (remotely)?
    - ➢ Access to the cloud should be routed through the agency's network; remote access must implement multi-factor authentication
    - ➢ Direct access to the cloud must occur after multi-factor authentication
- Incident Response
  - What happens when a cloud provider is breached or unauthorized disclosure occurs?
    - ➢ Agency must notify the appropriate Special Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA) and the IRS (immediately, no more than 24 hours)
- Onshore Services
  - Where can data be stored or accessed?
    - ➢ FTI may not be received, processed, stored or transmitted in offshore locations by any agency personnel

Cloud Security Considerations (Cont.)

- Service Level Agreements (SLAs)
  - Does the SLA with the Cloud Provider cover all requirements?
    - SLA must meet requirements stated under Section 5.5.2 and Exhibit 7 of IRS Publication 1075
    - SLA must state how the cloud provider will dispose of storage assets containing FTI
    - SLA must identify the cloud service model procured by the agency to help define agency-managed controls
- Media Protection
  - How is FTI labeled to facilitate awareness and potential forensic investigation?
    - In a database, FTI must be labeled at table level if not commingled and labeled at the element level if commingled
    - Documents must be identified as FTI
    - Data must not be available to other cloud tenants
- Risk Assessment
  - How does the agency assess risk of cloud implementation?
    - Periodic agency assessment must include magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of FTI and cloud systems

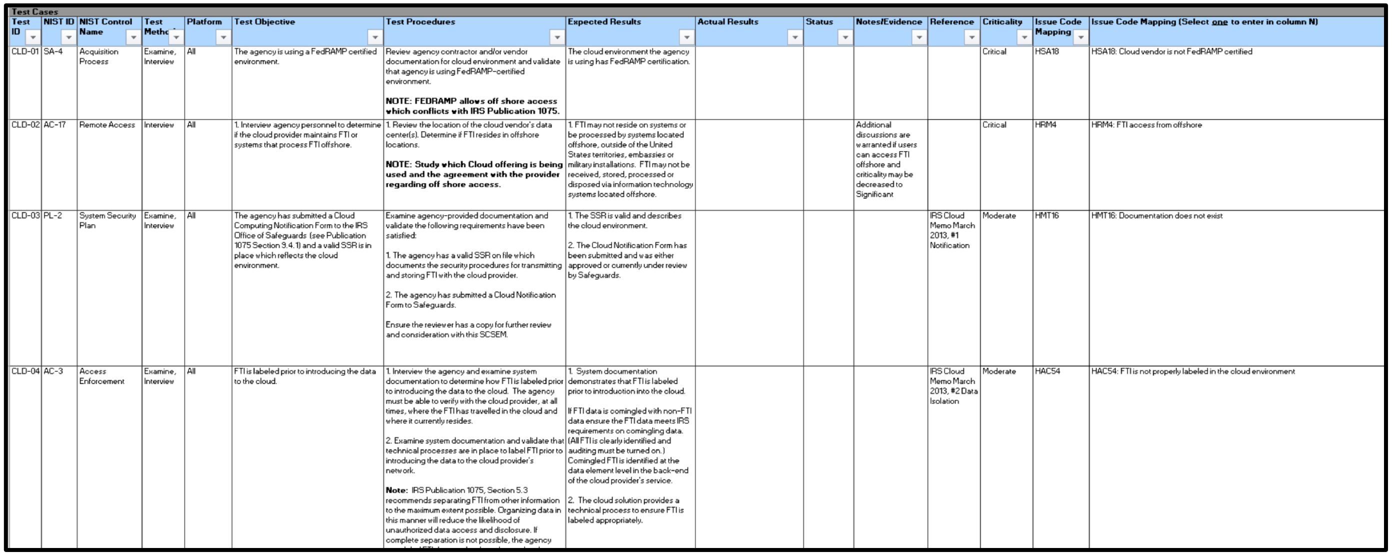
Cloud Security Considerations (Cont.)

- Encryption
  - Is encryption at rest required?
    - NIST SP 800-144 requires data at rest to be protected logically; data must be encrypted at rest to prevent unauthorized disclosure
    - Agency must specify the FIPS 140-2 compliant algorithm implemented (i.e. AES, 3DES with at least 128 bits in strength) to encrypt FTI at rest
- What are the requirements for encryption in transit?
  - Agency must specify the FIPS 140-2 compliant algorithm implemented (i.e. AES, 3DES with at least 128 bits in strength) to encrypt FTI in transit
- How should the agency control access to encryption keys?
  - Agency must retain sole ownership of keys such that cloud provider may not be able to access them when FTI type requires non-disclosure to contractors (e.g., (l)(7)TOP data)

Preparing for the On-Site Review of a Cloud Solution

Safeguards has released an updated Cloud Computing SCSEM which is available on the Safeguards website (www.irs.gov/uac/Safeguards-Program) in-line with the requirements listed in IRS Publication 1075 and other best practices.

- Safeguards has worked with Microsoft to create an Office 365 specific set of test cases and is working to finalize Azure test cases
- Safeguards is in contact with Google and Amazon to create additional solution-specific test cases
- More specific vendors and/or technologies may be added in the future



Test Cases

Test ID	NIST ID	NIST Control Name	Test Metho	Platform	Test Objective	Test Procedures	Expected Results	Actual Results	Status	Notes/Evidence	Reference	Criticality	Issue Code Mapping	Issue Code Mapping (Select <u>one</u> to enter in column N)
CLD-01	SA-4	Acquisition Process	Examine, Interview	All	The agency is using a FedRAMP certified environment.	Review agency contractor and/or vendor documentation for cloud environment and validate that agency is using FedRAMP-certified environment. **NOTE: FEDRAMP allows off shore access which conflicts with IRS Publication 1075.**	The cloud environment the agency is using has FedRAMP certification.					Critical	HSA18	HSA18: Cloud vendor is not FedRAMP certified
CLD-02	AC-17	Remote Access	Interview	All	1. Interview agency personnel to determine if the cloud provider maintains FTI or systems that process FTI offshore.	1. Review the location of the cloud vendor's data center(s). Determine if FTI resides in offshore locations. **NOTE: Study which Cloud offering is being used and the agreement with the provider regarding off shore access.**	1. FTI may not reside on systems or be processed by systems located offshore, outside of the United States territories, embassies or military installations. FTI may not be received, stored, processed or disposed via information technology systems located offshore.			Additional discussions are warranted if users can access FTI offshore and criticality may be decreased to Significant		Critical	HRM4	HRM4: FTI access from offshore
CLD-03	PL-2	System Security Plan	Examine, Interview	All	The agency has submitted a Cloud Computing Notification Form to the IRS Office of Safeguards (see Publication 1075 Section 9.4.1) and a valid SSR is in place which reflects the cloud environment.	Examine agency-provided documentation and validate the following requirements have been satisfied: 1. The agency has a valid SSR on file which documents the security procedures for transmitting and storing FTI with the cloud provider. 2. The agency has submitted a Cloud Notification Form to Safeguards. Ensure the reviewer has a copy for further review and consideration with this SCSEM.	1. The SSR is valid and describes the cloud environment. 2. The Cloud Notification Form has been submitted and was either approved or currently under review by Safeguards.				IRS Cloud Memo March 2013, #1 Notification	Moderate	HMT16	HMT16: Documentation does not exist
CLD-04	AC-3	Access Enforcement	Examine, Interview	All	FTI is labeled prior to introducing the data to the cloud.	1. Interview the agency and examine system documentation to determine how FTI is labeled prior to introducing the data to the cloud. The agency must be able to verify with the cloud provider, at all times, where the FTI has travelled in the cloud and where it currently resides. 2. Examine system documentation and validate that technical processes are in place to label FTI prior to introducing the data to the cloud provider's network. **Note:** IRS Publication 1075, Section 5.3 recommends separating FTI from other information to the maximum extent possible. Organizing data in this manner will reduce the likelihood of unauthorized data access and disclosure. If complete separation is not possible, the agency	1. System documentation demonstrates that FTI is labeled prior to introduction into the cloud. If FTI data is comingled with non-FTI data ensure the FTI data meets IRS requirements on comingling data. (All FTI is clearly identified and auditing must be turned on.) Comingled FTI is identified at the data element level in the back-end of the cloud provider's service. 2. The cloud solution provides a technical process to ensure FTI is labeled appropriately.				IRS Cloud Memo March 2013, #2 Data Isolation	Moderate	HAC54	HAC54: FTI is not properly labeled in the cloud environment

Preparing for the On-Site Review of a Cloud Solution

- Safeguards will evaluate SLAs, contracts, etc. established with the Service provider, in addition to evaluating security controls implemented by the agency. The nature of the agency-provided controls will depend on the Service Model in use.
- Safeguards has the following positions related to cloud computing:
  - If FTI is in a non-FedRAMP cloud, Safeguards will consider the cloud a critical finding.
  - If FTI is found to be offshore in the cloud environment, Safeguards will consider the cloud a critical finding.

FAQ

Q **Question 1:** Can we provide after hour / weekend Nessus scan results as part of our assessment?

A Scans must be performed during the onsite review hours and must be observed by a member of the IRS Safeguards team.

Q **Question 2:** Can we use an agency-provided Nessus license?

A Yes; in addition to the observation requirement, the agency must use Safeguards audit profiles and must provide the .Nessus, .csv, and .html output from each scan task.

Q **Question 3:** If our FTI is in a FedRAMP certified cloud, do the systems still need to be reviewed?

A Yes, at the very least the Cloud SCSEM will need to be reviewed during the onsite assessment. Based on the services provided, additional SCSEMs would be brought into scope.

Q **Question 4:** How can I limit the review of my third-party systems?

A Agencies may allow external information systems to connect to their environments through well-configured VDI as described in Publication 1075 section 9.4.13. Third-party systems strictly using VDI to gain access to the FTI systems are not included in the scope of a review.

FAQ

Q **Question 5:** Can I send our PFR and SRR to our consolidated data center POCs for remediation?

A Yes, the Safeguards Office will only provide reports directly to the agency. If only a portion of the CAP should be shared with a vendor or data center, an unlocked version can be requested from the Safeguards mailbox.

Q **Question 6:** Why were my IT department's workstation images included in the scope of the review? They do not access FTI.

A Administrator workstations are included in scope because they have access to systems where FTI is received, processed, stored, or maintained and could adjust the security features of those systems.

Q **Question 7:** Are machine certificates combined with a user password sufficient to meet Multi-Factor authentication requirements?

A The requirement for MFA remains having two of the three following factors satisfied during the authentication attempt:
-Something the user knows (e.g., a password)
-Something the user has (e.g., secure token)
-Something the user is (e.g., biometric information such as fingerprint)
Machine certificates combine something the user has (laptop with machine certificate) with something the user knows (password, to be entered into that machine) into the same authentication challenge, essentially nullifying the concept of multi-factor. Machine certificates are helpful for ensuring only approved devices attach to the network to satisfy IA-3, but are not sufficient for satisfying the requirements of AC-17, Remote Access.

Technical References

Document	Status	IRS Usage
NIST 800-144: Guidelines on Security and Privacy in Public Cloud Computing ***(May 2012)***	Final	Security Recommendations
NIST SP 800-145: The NIST Definition of Cloud Computing ***(September 2011)***	Final	Essential Characteristics Service Models Deployment Models
NIST 800-146: Cloud Computing Synopsis and Recommendations ***(May 2012)***	Final	Security Recommendations NIST 800-53 Families
NIST SP 500-291 v2: Cloud Computing Standards Roadmap ***(July 2013)***	Final	Criterion Selection
NIST SP 500-292: NIST Cloud Computing Reference Architecture ***(September 2011)***	Final	Taxonomy/Definitions

Technical References

Document	Status	Safeguards Usage
NIST SP 500-299: Evaluation of Cloud Computing Services Based on NIST SP 800-145 ***(N/A)***	Draft	Responsibilities
NIST SP 500-322: Evaluation of Cloud Computing Services Based on NIST SP 800-145 ***(February 2018)***	Final	Criterion Clarification Cloud Checklist
Cloud Security Alliance (CSA) Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 ***(July 2017)***	Final	Wealth of details

Department of the Treasury

Internal Revenue Service

www.irs.gov

IRS Office of Safeguards

www.irs.gov/uac/Safeguards-Program