Office of Privacy,
Governmental Liaison & Disclosure

IRS Safeguards

Office Hours

Topic: Cloud Computing with Federal Tax Information (FTI)

September 2018

Agenda

- What is a Cloud?
- Scoping Cloud Service Models
- Safeguards Requirements for Cloud Providers
- 45-Day Cloud Computing Notification
- Preparing for the on-site review of a cloud solution

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 such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction.

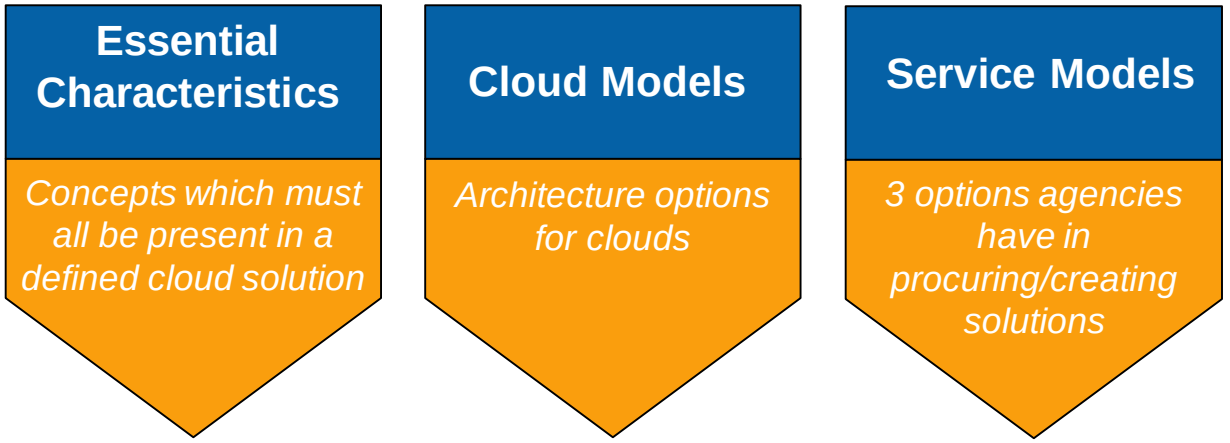
Determining a Cloud within the context of Safeguards

- The relationships between IRS, partner agencies, consolidated data centers and third parties may cause 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 such as the 45-Day Notification requirement and use of the 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 when an agency uses 3rd-party provided data storage and movement systems which meet cloud definition (multi-tenant, multiple facilities, etc.).	• **Contracted 3rd Party Services** such as 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

What is a Cloud?

- NIST SP 800-175 defines essential characteristics, cloud models and service model types for cloud computing.



- On Demand Self Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service

- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid Cloud

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

FedRAMP Authorization

FedRAMP

What is FedRAMP and its role?

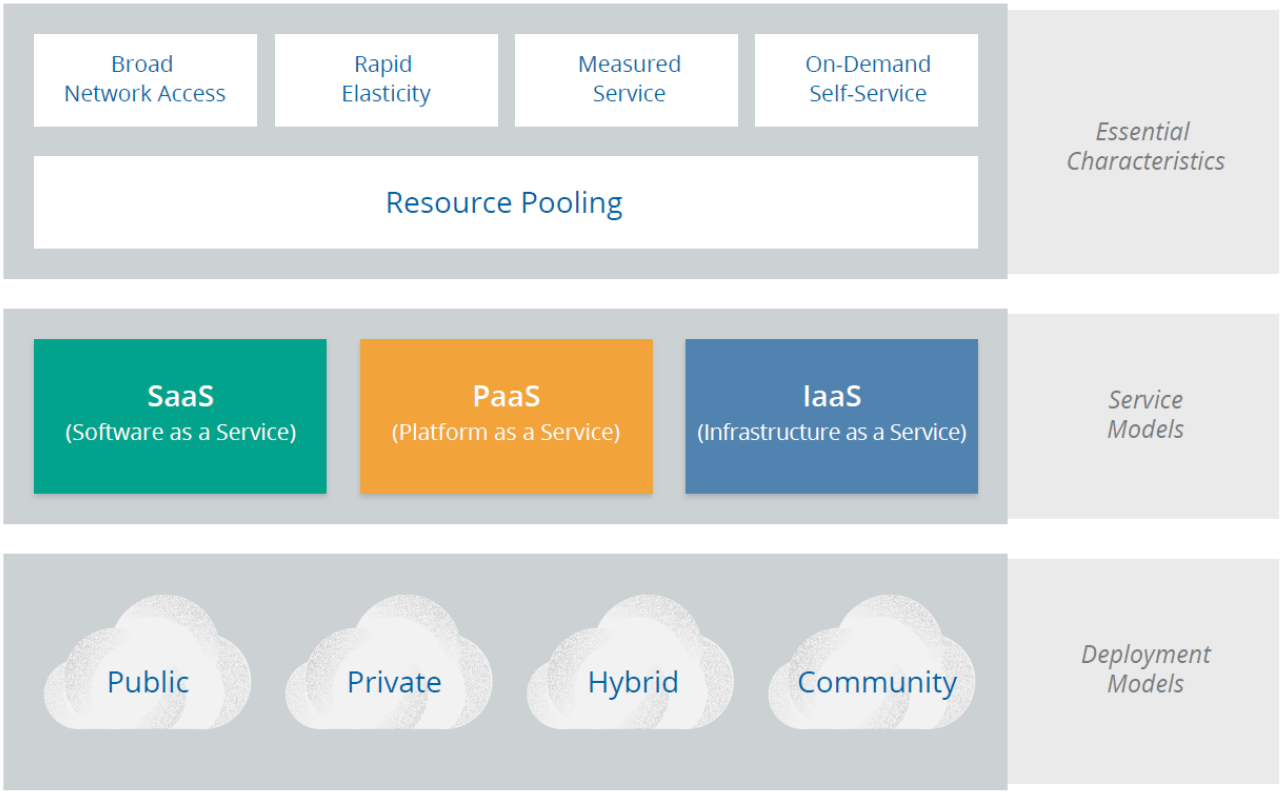
The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services.

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

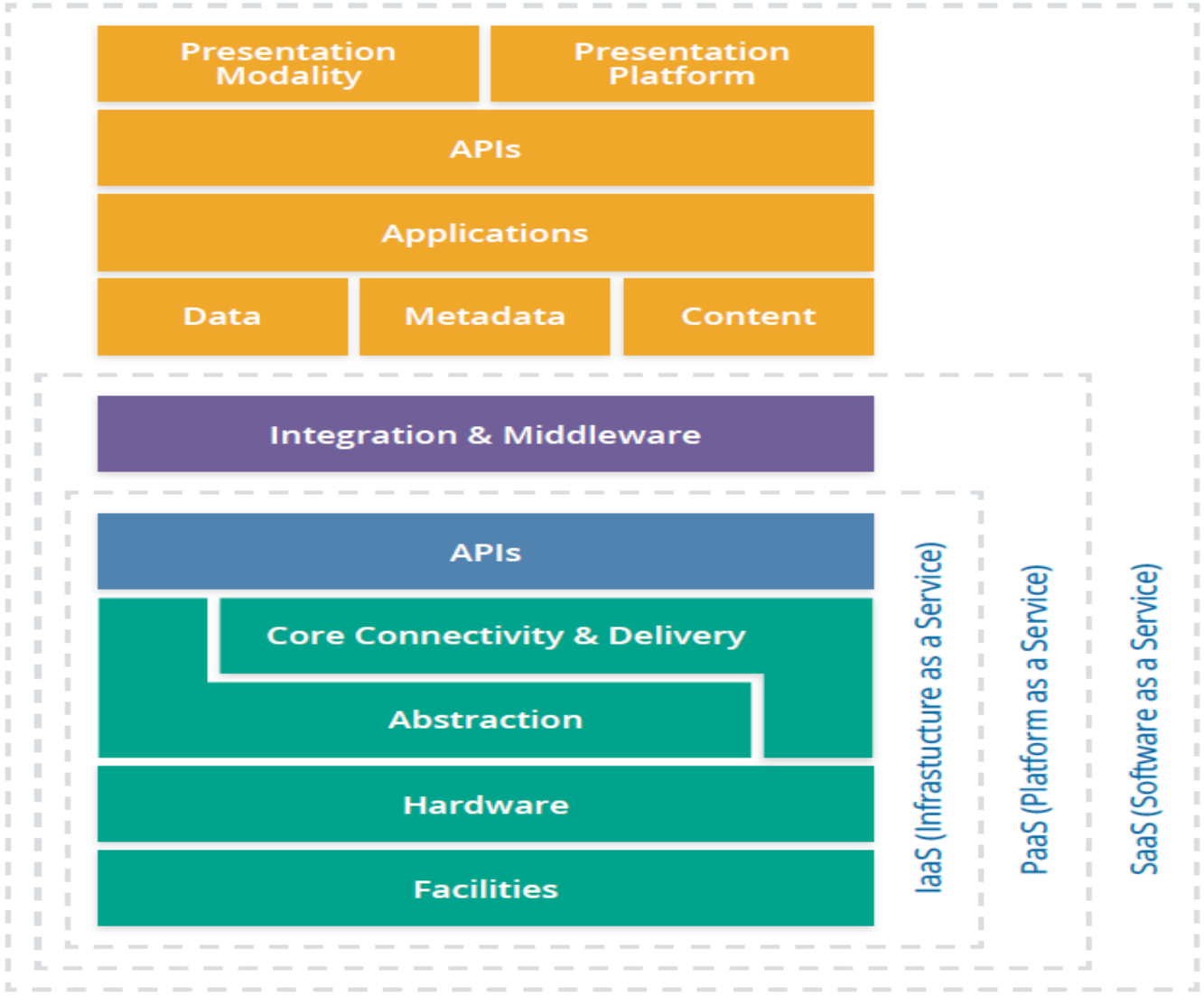
Cloud Basics

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



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 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

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

Safeguards Scoping Discussion:

- 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 comply with all Publication 1075 requirements. These are the mandatory requirements for introducing FTI to a cloud environment:

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

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 before transmitting FTI into a cloud environment.
- Find the Cloud Computing Notification form 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 United States
- 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?
    - Agency personnel may not receive, process, store or transmit FTI in offshore locations

Cloud Security Considerations (Cont.)

- Service Level Agreements (SLAs)
  - Does the SLA with the Cloud Provider cover all requirements?
    - SLA must comply with 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 and be encrypted 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 to its webpage (www.irs.gov/uac/Safeguards-Program) with requirements 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 more solution-specific test cases
- Safeguards may add other specific vendors and technologies.

Test Cases

Test ID	NIST ID	NIST Control Name	Test Method	Platform	Test Objective	Test Procedures	Expected Results	Actual Results	Status	Notes/Evidence	Reference	Criticality	Issue Code Mapping	Issue Code Mapping (Select one 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 3.4.1) 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 service level agreements and contracts set up with the provider as well as the agency's security controls. Agency-provided controls depend on the service model used.
- For cloud computing, Safeguards finds these situations critical:
  - 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.

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