ORACLE

Advisory: Oracle Cloud Infrastructure and Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies

Oracle Cloud Infrastructure US Government Cloud Regions and IRS Publication 1075

April 2022 | Version 1.0

Public

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. This document is not part of your agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you assessing your use of Oracle cloud services in the context of the requirements applicable to you under Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies. This information can also help you to assess Oracle as an outsourced service provider. You remain responsible for making your own independent assessment of the information in this document as the information in this document is not intended and cannot be used as legal advice about the content, interpretation or application of laws, regulations, and regulatory guidelines. Seek independent legal advice regarding the applicability and requirements of laws and regulations discussed in this document.

This document does not make any commitment to deliver any material, code, or functionality, and should not be relied on in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, is subject to periodic changes or revisions by the Internal Revenue Service. The current version Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, is available at irs.gov/pub/irs-pdf/p1075.pdf. This document is based on information available at the time of drafting. It is subject to change at the sole discretion of Oracle Corporation and may not always reflect changes in the regulations.

Table of Contents

Introduction

The US Internal Revenue Service Publication 1075 (IRS 1075) applies to all organizations that process or maintain US Federal Tax Information (FTI). Its purpose is to address any public request for sensitive information and prevent disclosure of data that would put FTI at risk. The IRS Office of Safeguards maintains Publication 1075, which provides guidance for policies, practices, controls, and safeguards for the protection of FTI to recipient agencies, agents, or contractors.

Document Purpose

This document is intended to provide relevant information related to Oracle Cloud Infrastructure (OCI) to assist you in determining the suitability of using OCI US Government Cloud in relation to IRS 1075. This document focuses on the mandatory requirements for FTI in a cloud environment as documented at irs.gov/privacy-disclosure/cloud-computing-environment. For full details, we recommend that you refer to IRS Publication 1075.

The information contained in this document does not constitute legal advice. Customers are advised to seek their own legal counsel to develop and implement their compliance program and to assess the features and functionality provided by Oracle regarding their specific legal and regulatory requirements.

About Oracle Cloud Infrastructure

Oracle's mission is to help customers see data in new ways, discover insights, and unlock possibilities. Oracle provides several cloud solutions tailored to customers' needs. These solutions provide the benefits of the cloud, including global, secure, and high-performance environments in which to run all your workloads. The cloud offerings discussed in this document include Oracle Cloud Infrastructure.

OCI is a set of complementary cloud services that enable you to build and run a wide range of applications and services in a highly available and secure hosted environment. OCI offers high-performance computing capabilities and storage capacity in a flexible overlay virtual network that's easily accessible from an on-premises network. OCI also delivers high-performance computing power to run cloud native and enterprise IT workloads. For more information about OCI, see docs.oracle.com/iaas/Content/home.htm.

The Cloud Shared Management Model

From a security management perspective, cloud computing is fundamentally different from on-premises computing. On-premises customers are in full control of their technology infrastructure. For example, they have physical control of the hardware and full control over the technology stack in production. In the cloud, however, customers use components that are partially under the management of the cloud service providers. As a result, the management of security in the cloud is a shared responsibility between the cloud customers and the cloud service provider.

Oracle provides best-in-class security technology and operational processes to secure enterprise cloud services. However, customers must also be aware of and manage their security and compliance responsibilities when running their workloads in OCI environments. By design, Oracle provides security functions for cloud infrastructure and operations, such as cloud operator access controls and infrastructure security patching. Customers are responsible for securely configuring and using their cloud resources. For more information, see the cloud service documentation at docs.oracle.com/iaas/Content/home.htm.

The following figure illustrates this division of responsibility at high level.

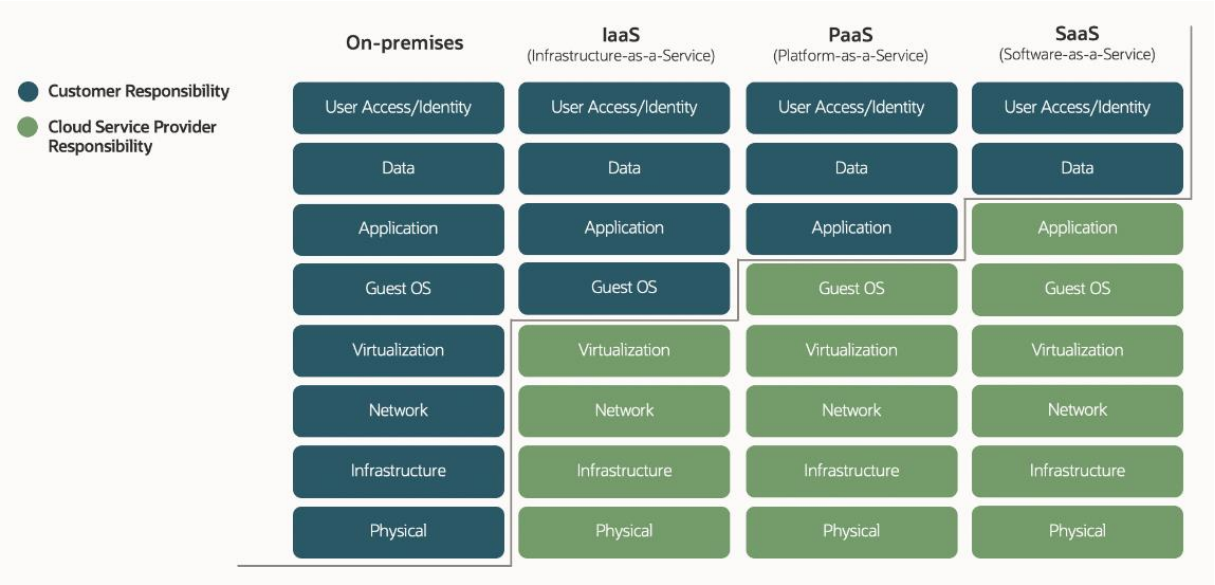

Figure 1: Conceptual Representation of the Various Security Management Responsibilities Between Customers and Cloud Providers

Mandatory Requirements for FTI in a Cloud Environment

The table in this section describes some of the OCI practices and controls in place to assist agencies in their evaluation of using OCI US Government Cloud for their FTI workloads. Customers are solely responsible for determining the suitability of a cloud service in the context of the existing mandatory requirements for FTI in a cloud environment. Customers are also responsible for ensuring that their use of the cloud service and their business processes meet these requirements.

REQUIREMENT	ORACLE PRACTICES
FedRAMP Authorization Cloud solutions used to receive, process or store must undergo a complete assessment using the FedRAMP Authorization Framework from an authorized third-party assessment organization (3PAO). The assessment must result in an Authority to Operate granted by the FedRAMP organization. Only FedRAMP-authorized solutions may receive, process, store or transmit FTI.	OCI US Government Cloud has been assessed by an independent third-party assessment organization and obtained Provisional Authority to Operate (P-ATO) from the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB). For a complete list of OCI US Government Cloud services that operate at FedRAMP High JAB, see marketplace.fedramp.gov/. Oracle has also engaged an independent third party, Schellman & Company, LLC, to assess OCI US Government Cloud controls for protecting FTI using the requirements from IRS 1075. The IRS 1075 controls were tested against applicable FedRAMP High control parameters. For more information, contact your Oracle account representative.
Onshore Access Agencies must leverage vendors and services where (i) all FTI physically resides in systems located within the United States; and (ii) all access and support of such data is performed from the United States. Identification of requirement that FTI may not be accessed by contractors located "offshore", outside of the United States or its territories. All physical locations where FTI is stored, transmitted, processed and/or received must remain within the United States. This includes all primary and secondary data centers and any backup facilities. Additionally, cloud environments (and any components, including, but not limited to, storage, virtualization, operating systems and networking) may not be accessed by vendor administrators from networks outside the United States. Further, FTI may not be received, stored, processed or disposed via information technology	Agencies choose the home region to locate their tenancy in. OCI's architecture means that data doesn't traverse regions unless the customer allows it. Use of OCI US Government Cloud regions ensures that systems, data, operations, and support is performed within the US. For more information about Oracle Cloud data regions, see oracle.com/cloud/cloud-regions/.

REQUIREMENT	ORACLE PRACTICES
systems located off-shore. The discovery of offshore storage and/or access to FTI during an onsite Safeguards review will result in a Critical finding.	
Physical Description Agencies and their cloud providers must provide a complete listing of all data centers within the cloud environment where FTI will be received, processed, transmitted or stored. In addition to certifying all data centers, environments and equipment reside onshore, the agency and provider must disclose all physical locations where FTI is received, processed, stored and maintained. Safeguards cannot approve the implementation of cloud solutions without a full understanding of the physical locations where FTI is processed, in addition to understanding the logical protections the solution provides.	Agencies choose the home region to locate their tenancy in. OCI's architecture means that data doesn't traverse regions unless the customer allows it. For more information about the location of OCI US Government Cloud data centers, see the following resources: • docs.oracle.com/iaas/Content/General/Concepts/govfedramp.htm • oracle.com/cloud/data-regions/#government • oracle.com/cloud/cloud-regions/
45-Day Notification The agency must notify the IRS Office of Safeguards at least 45 days prior to transmitting FTI into a cloud environment. To utilize a cloud environment that receives, processes, stores or transmits FTI, the agency must meet the following mandatory notification requirement: • The agency must submit a Cloud Computing Notification (see Publication 1075 Section 9.4.1, Cloud Computing Environments) to the IRS Office of Safeguards at least 45 days prior to transmitting FTI into a cloud environment.	The agency is solely responsible for meeting this requirement.
Data Isolation Software, data and services that receive, transmit, process or store FTI must be isolated within the cloud environment so that other cloud customers sharing physical or virtual space cannot access other customer data or applications. IRS Publication 1075, section 5.2, Commingling of FTI, 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 must label FTI down to the data element level. Labeling must occur prior to introducing the data to the cloud and the data must be tracked accordingly through audit trails captured for operating systems, databases and applications that receive, store, process or transmit FTI. IRS Publication 1075, section 9.3.3, Audit & Accountability, states audit logs must enable tracking activities taking place on the system. It also contains requirements for creating audit-related processes at both the application and system levels. Within the application, auditing must be enabled to the extent necessary to capture access, modification, deletion and movement of FTI by each unique user. This auditing requirement also applies to data tables or databases embedded in or residing outside of the application. Included in that section, as well, is the requirement for agencies to "coordinate the access and protection of audit information" with its cloud providers.	OCI's infrastructure and its security and management tools are isolated both physically and logically. OCI uses *enclaves*, which means that customer space and OCI internal services are on physically separate machines and are logically separated by network access control lists (ACLs) that prohibit unauthorized connections between the enclaves. OCI security and management services' network traffic is also encapsulated and encrypted using NSA-approved algorithms and parameters. For more information, see the Oracle Cloud Hosting and Delivery Policies at oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf. Agencies can also use OCI services such, as Audit and Identity and Access Management (IAM), to track access to FTI stored on OCI.

REQUIREMENT	ORACLE PRACTICES
Service Level Agreements (SLA) and Contracts The agency must establish security policies and procedures based on IRS Publication 1075 for how FTI is stored, handled and accessed inside the cloud through a legally binding contract or SLA with their third-party cloud provider. While the agency may not have direct control over FTI at all times, they ultimately maintain accountability while it is in the cloud, and the ownership rights over the data must be firmly established in the service contract to enable a basis for trust. The SLA is a mechanism to mitigate security risk that comes with the agency's lack of visibility and control in a cloud environment. It is important that agencies establish SLAs with cloud providers that clearly identify Publication 1075 security control requirements and determine who has responsibility (provider, customer) for their implementation. At a minimum, SLAs with cloud providers must include: • IRS Publication 1075, Exhibit 7 contract language; • Identification of computer security requirements the cloud provider must meet per IRS Publication 1075, section 9, Computer System Security, which provides the security control requirements to include in agreements with third-party cloud providers; • Identification of requirements for cloud provider personnel who have access to FTI. All cloud provider personnel with logical FTI access must have a justifiable need for that access and submit to a background investigation; • Identification of requirements for incident response to ensure cloud providers follow the incident notification procedures required by IRS Publication 1075. In the event of an unauthorized disclosure or data breach, the cloud provider and agency must report incident information to the appropriate Agent-in-charge, TIGTA and the IRS Office of Safeguards within 24 hours according to Publication 1075, section 10, Reporting Improper Inspections or Disclosures; • Agreement on the scope of the security boundary for the section of the cloud where FTI is accessible and systems with FTI reside. The agency must ensure that boundary details are included in the SLA between the two parties; • Clearly state that agencies have the right to require changes to their section of the cloud environment and cloud providers will comply with IT policies and procedures provided by the agency; • IRS Publication 1075, Exhibit 6, Contractor 45-day Notification Procedures contains a requirement for notifying the IRS prior to executing any agreement to disclose FTI to a contractor the cloud provider may utilize, or at least 45 days prior to the disclosure of FTI, to ensure appropriate contractual language is included and that contractors are held to safeguarding requirements and • Identification of cloud provider employee awareness and training requirements for access to FTI and incident response. IRS Publication 1075, 6.2, Training Requirements states employees must be certified to understand the agency's security policy and procedures for safeguarding IRS information prior to being granted access to FTI, and must maintain their authorization to access FTI through annual recertification.	Oracle has standard contracts and policies that govern the terms, service descriptions, and delivery of cloud services. To find out more about these contracts and policies, see oracle.com/corporate/contracts/cloud-services/contracts.html. The Oracle Internal Revenue Service Publication 1075 Addendum includes IRS 1075 Exhibit 7 Safeguarding Contract Language. The addendum can be used with the Ordering document for OCI infrastructure and platform as a service (IaaS and PaaS). For more information, contact your Oracle account representative. As a cloud service provider, Oracle generally has no insight into the data that customers store or process in OCI or if it's FTI. Oracle lists its strategic subcontractors on My Oracle Support (Doc ID 2667492.2). The agency can sign up to receive notification or any updates to this document. To obtain a list of strategic subcontractors specific to your tenancy, contact your account representative.

REQUIREMENT	ORACLE PRACTICES
Data Encryption in Transit FTI must be encrypted in transit 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. This requirement must be included in the SLA. IRS Publication 1075 requires encryption of FTI in transit in Section 9.3.16.6, Transmission Confidentiality and Integrity (SC-8). The agency must ensure that encryption requirements are included in contracts with third-party providers. The IRS does not advocate specific mechanisms to accomplish encryption as long as they are FIPS 140-2 compliant and configured securely. Additionally, agencies must retain control of the encryption keys used to encrypt and decrypt the FTI at all times and be able to provide information as to who has access to and knows information regarding the key passphrase.	Oracle implements technical controls designed to protect the confidentiality, integrity, and availability of corporate information assets, including secure configurations and encryption for data in transit. Unique encryption keys are created for each customer when their tenancy is created, and these keys are stored in a FIPS 140-2 Level 3 validated hardware security module (HSM). Customers can also choose to provide their own encryption keys instead of using OCI-provisioned keys to protect their data in OCI's storage systems and database services. For Compute systems, the customer is required to provide their own SSH key for establishing connection to hosts in OCI. The OCI Vault service allows customers to manage keys within a physical HSM managed by OCI. These keys can be used to protect data within OCI storage services if they are explicitly authorized to do so by the customer. The OCI Object Storage, Block Volume, File Storage, and Streaming services integrate with the Vault service to support encryption of data in buckets, block or boot volumes, file systems, and stream pools. For more information about the Vault service, see docs.cloud.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htm.
Data Encryption At Rest FTI must be encrypted while at rest in the cloud using a NIST-validated, FIPS 140-2 compliant encryption module. Encryption protects the confidentiality and integrity of the data and provides a methodology for segmenting an agency's data from others while stored. This requirement must be included in the SLA. In a cloud environment, protection of data and data isolation are a primary concern. Encryption of data at rest provides the agency with assurance that FTI is being properly protected in the cloud. NIST's SP 800-144 recommends, "Data must be secured while at rest, in transit and in use, and access to the data must be controlled." The IRS does not advocate specific mechanisms to accomplish encryption as long as they are FIPS 140-2 compliant and configured securely. Additionally, agencies must retain control of the encryption keys used to encrypt and decrypt the FTI at all times and be able to provide information as to who has access to and knows information regarding the key passphrase. If the agency is able to satisfy this requirement, effectively preventing logical access to the data from the cloud vendor, agencies may use cloud infrastructure for data types that have contractor-access restrictions.	Oracle implements technical controls designed to protect the confidentiality, integrity, and availability of corporate information assets, including secure configurations and encryption for data at rest. Unique encryption keys are created for each customer when their tenancy is created, and these keys are stored in a FIPS 140-2 Level 3 validated HSM. Customers can also choose to provide their own encryption keys instead of using OCI provisioned keys to protect their data in OCI's storage systems and database services. For Compute systems, the customer is required to provide their own SSH key for establishing connection to hosts in OCI. The OCI Vault service allows customers to manage keys within a physical HSM managed by OCI. These keys can be used to protect data within OCI storage services if they are explicitly authorized to do so by the customer. The OCI Object Storage, Block Volume, File Storage, and Streaming services integrate with the Vault service to support encryption of data in buckets, block or boot volumes, file systems and stream pools. For more information about the Vault service, see docs.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htm. Oracle Database security capabilities include transparent data encryption (TDE). For more information about database security, see docs.oracle.com/iaas/Content/Security/Reference/dbaas_security.htm. As cloud provider, Oracle generally has no logical access to the data that agencies store or process in OCI.

REQUIREMENT	ORACLE PRACTICES
Persistence of Data in Relieved Assets Storage devices where FTI has resided must be securely sanitized and/or destroyed using methods acceptable by National Security Agency/Central Security Service (NSA/CSS). This requirement must be included in the SLA. If a storage device fails, or in situations where the data is moved within or removed from a cloud environment, actions must be taken to ensure residual FTI is no longer accessible. The destruction or sanitization methods apply to both individual devices that have failed as well as in situations where the agency removes data from the cloud environment or relocates FTI to another environment. As there are varied approaches towards secure sanitization based on provider specifications, cloud providers should consult their data storage provider to determine the best method to sanitize the asset. If the storage device will no longer be in service, the residual data must be purged using Secure Erase or through degaussing using a NSA/CSS approved degausser. The cloud provider is required to notify the agency upon destroying or repurposing storage media. The agency must verify that FTI has been removed or destroyed and notify the IRS Office of Safeguards of the destruction of storage media in the agency's annual Safeguard Security Report (SSR).	The Oracle Internal Revenue Service Publication 1075 Addendum includes IRS 1075 Exhibit 7 Safeguarding Contract Language, which includes storage devices destruction requirements. Oracle's Media Sanitation and Disposal Policy defines requirements for the removal of information from electronic storage media (sanitization), and disposal of information that's no longer required, either in hard copy form or on electronic storage media, so that the information is protected from security threats associated with retrieval and reconstruction of confidential data. Electronic storage media include laptops, hard drives, storage devices, and removable media, such as tape. The Cloud Compliance Standard for Asset Management includes procedures for asset retirement and removal and require that storage systems are wiped in accordance with NIST 800-88 Rev. 1 before release or disposal.
Risk Assessments The agency must conduct an annual assessment of the security controls in place on all information systems used for receiving, processing, storing and transmitting FTI. The IRS Office of Safeguards will evaluate the risk assessment as part of the 45 Day notification requirement. Agencies are required to conduct a risk assessment (or update an existing risk assessment, if one exists) when migrating FTI to a cloud environment. Subsequently, the risk assessment must be reviewed annually to account for changes to the environment. The implementation and an evaluation of the associated risks should be part of the risk assessment. The IRS Office of Safeguards will evaluate the risk assessment as part of the above notification requirement.	The agency is solely responsible for meeting this requirement. The Oracle Internal Revenue Service Publication 1075 Addendum provides for the inspection of the services provided by OCI, including alignment with NIST 800-53 Rev. 5 controls. The OCI Risk and Resilience team is responsible for identifying, analyzing, measuring, mitigating, responding to, and monitoring risk specific to the OCI organization. Risk assessments are performed annually across OCI to identify threats and risks that could impact the security, confidentiality, or availability of the system. The risk assessment is modeled after NIST Special Publication 800-30 Rev. 1 guidelines and incorporates risk assessment requirements from the ISO/IEC 27001:2013 standard. OCI's risk management assessment program documentation is examined by a third-party assessor under the bi-annual System and Organization Controls (SOC) audit program.
Multi-Factor Authentication Cloud implementations which truly represent remote access from the internet must incorporate multi-factor authentication. • Remote access to the cloud where the access is available over the public internet requires multi-factor authentication. Multi-factor authentication requires at least two of the three criteria: 1) something a user knows (e.g., password); 2) something a user has (e.g., hardware cryptographic token) and 3) something a user is (e.g., using biometric information).	The agency is solely responsible for implementing multi-factor authentication (MFA) in its environment, specifically regarding remote access of FTI. Agencies can use OCI services, such as Identity and Access Management (IAM), to manage MFA in OCI. For more information, see docs.oracle.com/iaas/Content/Identity/Tasks/usingmfa.htm. Oracle defines the logical access control requirements for all Oracle systems—including authentication, authorization, access approval, provisioning, and revocation—for employees and any other Oracle-defined users with access to Oracle systems that aren't internet-facing, publicly accessible systems. OCI policies and procedures have established security controls in support of MFA. Two factors work together, requiring an extra layer of security to verify the user's identity and complete the sign-in process.

REQUIREMENT	ORACLE PRACTICES
Security Control Implementation Customer defined security controls must be identified, documented and implemented. The customer defined security controls, as implemented, must comply with Publication 1075 requirements. Cloud providers may designate selected controls as customer defined. For customer defined security controls, the agency must identify, document and implement the customer defined controls, in accordance with Publication 1075. Implementation of some controls may need to be done in partnership with the agency's cloud provider, however the agency has primary responsibility for ensuring it is completed. The agency's capability to test the functionality and security control implementation of a subsystem within a cloud environment is more limited than the ability to perform testing within the agency's own infrastructure. However, other mechanisms such as third-party assessments may be used to establish a level of trust with the cloud provider.	The agency is solely responsible for meeting this requirement. OCI security controls are regularly tested by an independent third-party assessor. The resulting reports and certifications are made available to customers in the Oracle Cloud Console. For more information, see the following resources: • docs.oracle.com/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm • oracle.com/corporate/cloud-compliance/

Conclusion

IRS Publication 1075 provides security guidelines for federal, state, and local agencies for protecting FTI. With Oracle Cloud Infrastructure US Government Cloud services, Oracle provides many features that can help you achieve your compliance objectives.

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle