Starting your accreditation journey with Oracle Cloud for US Government

Understanding Oracle Cloud Infrastructure regions and compliance

Table of Contents

Disclaimer

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

This document is intended to outline our general product direction. It is intended for information purposes only and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Preface

This document helps commercial entities interested in using Oracle Cloud Infrastructure (OCI) US Government cloud better understand the relationship of NIST SP 800-53 controls and various security requirements, standards, certifications, and authorizations such as FedRAMP and CMMC.

Introduction

Security is the top priority for US Government information technology which has led to multiple requirements that commercial entities may need to satisfy to achieve accreditation with the US Government. IT security is not the same as compliance. IT *security* is about protecting access to services and data, while *compliance* is the demonstration of those protective actions. Compliance is more than demonstrating a security posture at a single point in time. It requires following processes for continuous monitoring and evaluation of systems to maintain security over time. These control efforts include documenting, informing, validating, and *demonstrating* what actions you have taken to protect your services and data. Compliance, including US Government authorizations and certification, are designed to demonstrate you have achieved these security controls.

The National Institute of Standards and Technology (NIST) has detailed hundreds of security controls and compliance standards to protect cloud solutions. These security controls form the basis of most government cloud compliance standards. These compliance standards are often verified by an independent third-party auditor organization (3PAO). Therefore, when someone says a solution has achieved a specific compliance standard, that indicates which controls have been achieved and that a non-biased party has validated that achievement.

Some accreditations offer reciprocity from other accreditations. For example, if a solution achieves Federal Risk and Authorization Management Program (FedRAMP) accreditation, that likely means it has also achieved the Texas Risk and Authorization Management Program (TX-RAMP), though not necessarily the other way around. FedRAMP is viewed as the top-level standard of government compliance achievement for US federal, civilian, state and local, and commercial entities. Defense Information Systems Agency (DISA) Impact Level (IL) is the standard for US Department of Defense and intelligence agencies. Both are built on the foundation of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 controls, and both have multiple levels.

NIST SP 800-53 is Special Publication series 800 and the requirements are mandated by the Federal Information Security Management Act (FISMA) and outlined by the Federal Information Processing Standards (FIPS). NIST SP 800-53 is specific to federal networks, while NIST SP800-171 applies to non-federal networks.

These NIST frameworks have three levels based on organizational impact risk – low, moderate, and high.

- **Low impact:** There are limited adverse effects on an organization's operations, assets, or individuals (e.g., minor damage to organization assets, minor harm to individuals or minimal financial loss).
- **Moderate impact:** There are serious adverse effects to organization operations, assets, or individuals (e.g., significant damage to organizational assets, financial loss or harm to individuals).
- **High impact:** There are severe or catastrophic impacts to organization operations, assets, or individuals (e.g., loss of life or life-threatening injuries to individuals, financial loss or major damage to organizational assets).

Security Controls

FedRAMP requires security compliance for secure code, people, processes, tools, availability, and the physical infrastructure. Within each impact level there are controls spanning 18 cloud security domains:

1. Access Control
2. Audit and Accountability
3. Awareness and Training
4. Configuration Management
5. Contingency Planning
6. Identification and Authentication
7. Incident Response
8. Maintenance
9. Media Protection
10. Personnel Security
11. Physical and Environmental Protection
12. Planning
13. Program Management
14. Risk Assessment
15. Security Assessment and Authorization
16. System and Communications Protection
17. System and Information Integrity
18. System and Services Acquisition

Types of Accreditations

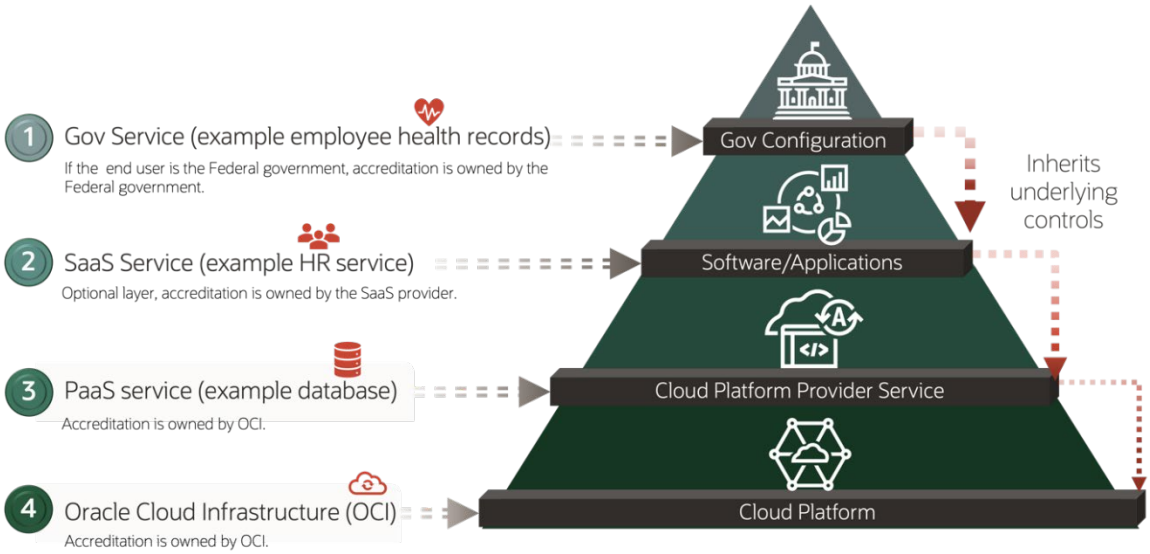
In addition to FedRAMP, there are many more US Government compliance standards, including:

1. DISA IL – Defense Information Systems Agency Impact Level
2. ITAR – International Traffic in Arms Regulations
3. CJIS – Criminal Justice Information Services
4. IRS1075 – Internal Revenue Service Publication 1075 Tax Information Security Guidelines
5. CMMC – Cybersecurity Maturity Model Certification
6. FISMA – Federal Information Security Management Act
7. State-RAMP – State Risk and Authorization Management Program
8. TX-RAMP – Texas Risk and Authorization Management Program

The accreditations you may need to pursue will likely be driven by your type of organization, your end users, and what type of solution you are providing. Not all accreditations may be applicable to all providers or all solutions, so it is your responsibility to understand which are relevant to you and your end users.

FedRAMP

FedRAMP is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. There are four tiers of FedRAMP Authority to Operate (ATO) for cloud accreditation. Tier 2 is only applicable to those offering Software as a Service (SaaS).



In addition to these four tiers, FedRAMP has three levels of requirements that apply to both federal agencies and cloud providers. If FedRAMP High is achieved, that level includes the Low and Moderate level control requirements, which means the achievement is additive, not separate (i.e., if you achieve Moderate, then by definition you have also achieved Low). The three FedRAMP levels align to the impact levels listed above previously:

- **Low:** 125 controls
- **Moderate:** 325 controls
- **High:** 421 controls

**Please note: An agency may be able to require additional controls above FedRAMP requirements based on their risk management practices.*

Federal agency accreditation:

Federal agencies may also need to achieve an ATO before their service may be provided to its designated user community in a production environment. Even if an agency builds a solution on top of a FedRAMP accredited Cloud Service Provider (CSP) offering, the agency is still required to obtain an ATO from the agency's authorizing official. This document is not authored for government agencies but meant to help commercial entities understand requirements they should meet when providing services to the government.

Cloud Service Provider accreditation:

There are 2 types of FedRAMP authorization a CSP may achieve: Agency and Joint Authorization Board (JAB).

FedRAMP agency accreditation

FedRAMP agency authorization denotes achieving an ATO with a single specific agency, and it is that federal agency that has reviewed and approved a CSP service. CSPs should have a US federal government sponsoring agency to achieve agency authorization. This means that a CSP who only serves state and local government users cannot get an agency accreditation. This ATO is solution and implementation specific.

FedRAMP JAB accreditation

FedRAMP JAB accreditation may be perceived as superior to an agency accreditation because it is reviewed by the JAB which includes multiple agencies. The JAB collectively reviews with more varied use cases in mind while evaluating the same FedRAMP controls.

The JAB is made of a designee assigned by the Chief Information Officers from the Department of Defense (DoD), the Department of Homeland Security (DHS), and the General Services Administration (GSA). The JAB may only offer a provisional ATO (P-ATO) based on the boundary and services identified in the submission. The final authority to operate (ATO) will be approved by the agency authorizing official.

It is also important to understand that any single vendor may need to achieve multiple authorizations, including authorizations for each cloud service. There may be an authorization for Infrastructure as a Service (IaaS), each individual Platform as a Service (PaaS), and each individual software as a Service (SaaS). A service cannot achieve authorization by simply running on an authorized IaaS. Authorization is required to confirm controls are in place to implement the FedRAMP requirements for each service. PaaS typically has inherited controls from IaaS, with more applicable controls based on the service functionality. SaaS also inherits controls from IaaS, with more applicable controls based on the service functionality. It is common for IaaS, PaaS, and SaaS to have shared controls within the cloud shared responsibility model.

The stages for authorization are the same for both Agency and JAB, but there are different activities within each stage:

STAGE	AGENCY	JAB
Preparation	Readiness Assessment and Pre-Authorization. "In Process" Designation possible	FedRAMP Connect Readiness Assessment Full Security Assessment
Authorization	Full Security Assessment and Agency Authorization Process. "Authorized" Designation once complete	JAB Authorization Process "In Process" Designation "Authorized" Designation once complete
Continuous Monitoring	Ongoing Continuous Monitoring Deliverable and an Annual Assessment	Ongoing Continuous Monitoring Deliverable and an Annual Assessment

Defense Information Systems Agency (DISA) Impact Level (IL)

The Department of Defense (DoD) through Defense Information Systems Agency (DISA) has created the Cloud Computing Security Requirements Guide (CCSRG) to assist the DoD in selecting a CSP and assuring that the proper security controls have been achieved. CCSRG describes the basis for the DoD security posture, defines policies, requirements, and architectures. The CCSRG guides DoD mission owners on how to use a Cloud Service Offering (CSO). The goal is to create a framework that defines requirements that allow the Mission Owner to achieve ATO. There are 4 Impact Levels - IL 2, 4, 5, and 6 - based on the sensitivity of the information stored or processed in the cloud and the impact that could result in the loss of confidentiality, integrity, or availability of that data.

IL 2 is designed for DoD information that has been approved for public release (note: IL2 may be achieved through reciprocity of FedRAMP Moderate). IL4 is for Controlled Unclassified Information (CUI) that is For Official Use Only (FOUO). IL5 is for CUI and National Security Systems. IL6 is for Classified Information up to secret level.

DISA grants a Provisional Authorization to Mission Owners for CSOs when they demonstrate their unique configuration and code when combined with the offerings from a CSP have demonstrated compliance with the CCSRG. The DISA IL control base is very similar to FedRAMP, and IL4 will accept FedRAMP High accreditation as a basis for a Provisional Authorization. IL5 requires a connection to the DISA NIPRNet via the BCAP or DREN. The primary difference between the OCI US Government cloud and the OCI US DoD cloud is that the DoD cloud has NIPRNet connectivity, and the US Government cloud does not.

International Traffic in Arms Regulations (ITAR)

Customers with International Traffic in Arms Regulations (ITAR) compliance requirements need to know what is required of their cloud implementation. ITAR, administered by the Directorate of Defense Trade Controls (DDTC) within the US State Department, regulates the manufacture, sale, and distribution of defense and space-related articles and services. US Government agencies and contractors that need to store, manage, and access ITAR data in a cloud environment need to ensure that specific controls are in place to meet their regulatory obligations. ITAR requires that only US persons have physical or logical access to the items on the United States Munitions List (USML). US persons may be US citizens or US Green Card (Permanent Resident Card) holders. Review the list below to determine if ITAR applies to your business operations. The USML includes the following 21 categories of defense articles and more detail may be found on the ITAR website.

1. Firearms and Related Articles
2. Guns and Armament
3. Ammunition and Ordnance
4. Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs, and Mines
5. Explosives and Energetic Materials, Propellants, Incendiary Agents and Their Constituents
6. Surface Vessels of War and Special Naval Equipment
7. Ground Vehicles
8. Aircraft and Related Articles
9. Military Training Equipment and Training
10. Personal Protective Equipment
11. Military Electronics
12. Fire Control, Laser, Imaging, and Guidance Equipment
13. Materials and Miscellaneous Articles
14. Toxicological Agents, Including Chemical Agents, Biological Agents, and Associated Equipment
15. Spacecraft and Related Articles
16. Nuclear weapons Related Articles
17. Classified Articles, Technical Data, and Defense Services Not Otherwise Enumerated
18. Directed Energy Weapons
19. Gas Turbine Engines and Associated Equipment
20. Submersible Vessels and Related Articles
21. Articles, Technical Data, and Defense Services Not Otherwise Enumerated

OCI US Government cloud authorizations and customer's responsibility for ITAR data

As of January 1, 2023 (please check periodically for any updates to ITAR requirements), there are no formal ITAR compliance certifications available for IaaS and PaaS cloud providers, however the OCI US Government cloud is continuously audited by an accredited independent 3PAO for FedRAMP. As a FedRAMP High JAB-authorized

service, OCI US Government Cloud offers in-scope cloud services that meet or exceed the requirements of FedRAMP High level, and our customer's environment may be able to inherit select controls that OCI maintains. OCI US Government cloud provides a physically and logically isolated environment supported and managed by trained US persons located exclusively within the United States. All customer data remains in-country unless our customers proactively move it elsewhere.

OCI IaaS and PaaS services make it easy for government agencies and approved contractors to digitally transform legacy mission systems securely, efficiently, and effectively. Customers may successfully migrate their workloads to OCI US Government Cloud, knowing that OCI maintains compliance with US federal security requirements, such as FedRAMP High and DISA IL4 and IL5 as a foundation for the pursuit of managing ITAR data.

Criminal Justice Information Services (CJIS)

The Criminal Justice Information Services (CJIS) division of the US Federal Bureau of Investigation (FBI) was established in 1992. The CJIS Security Policy establishes standards for data security and encryption for professionals in criminal justice and law enforcement at the local, state, and federal levels. Criminal Justice Information (CJI) data includes information for detaining criminals, performing background checks, and tracking criminal activity.

CJIS devised a set of standards to ensure cybersecurity best practices concerning wireless networks, remote access, data encryption, and multiple-step authentication. The primary goal of the CJIS Security Policy is to provide appropriate controls to protect the entire lifecycle of CJI, whether at rest or in transit.

The CJIS Security Policy defines 13 policy areas that CSPs should evaluate to determine if their use of cloud services adheres to CJIS requirements. These areas relate to NIST 800-53, the basis for FedRAMP. With the implementation of FedRAMP requirements, Oracle Government Cloud recognizes in-scope cloud services meet or exceed the requirements of many security standard controls.

The CJIS Security Policy requires multiple security controls that ensure that only authorized individuals have access to CJI. OCI provides building blocks that public safety agencies may use to build highly available and secure applications to meet the policy requirements. One foundational element of the CJIS Security Policy is the principle of least privilege, which is based on a "need-to-know, right-to-know" standard. Oracle customers may enforce this standard by securely encrypting their CJI and limiting access to this information to only those with access to the encryption keys. Oracle also provides data masking and subsetting options within Oracle databases which help obfuscate data to aid in designing data protection policies.

At this time of this publication, no formal third-party assessed CJIS compliance program exists for IaaS and PaaS providers to certify or authorize their standalone offering. Oracle US Government Cloud is continuously audited by an accredited independent 3PAO for FedRAMP. Customers should demonstrate CJIS compliance and accredit the solutions that they build in OCI. Because data is owned by the customer, it is not under the cloud provider's responsibility to influence or manage controls.

Internal Revenue Service (IRS) 1075

IRS 1075 exists to ensure the proper practices and safeguards are in place to protect the confidentiality and unauthorized use of personal and financial information furnished to the IRS. The intent is to allow data exchange within and potentially between agencies, while preventing the inappropriate disclosure of Federal Tax Information (FTI). Customers need to understand how controls defined in IRS 1075 apply to cloud computing providers, how they may leverage proven controls audited by a 3PAO, and how to be accredited by FedRAMP.

IRS 1075 applies to all organizations that transmit, process, or maintain US FTI. The intent 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 IRS 1075 which provides guidance for policies, practices, controls, and safeguards for the protection of FTI to recipient agencies, agents, or contractors. IRS 1075 compliance may only be achieved by the government agency or commercial customer processing or storing FTI. Customers may rely on controls OCI has accredited through FedRAMP certification within the shared responsibility model.

IRS 1075 is not a certification that an IaaS/PaaS CSP may achieve because the CSP is not responsible for all the controls that are required under IRS 1075. CSPs like Oracle may support IRS 1075 compliance by offering cloud services with demonstration of implemented controls. For example, OCI has achieved FedRAMP High P-ATO which demonstrates NIST SP 800-53 controls have been tested and are operating effectively. Agencies maintaining FTI in a cloud environment should use a CSP that has achieved FedRAMP certification. The end-user solution provider may use these proven controls, reducing the effort to ensure their overall solution is compliant.

OCI US Government cloud offers several key security practices that may assist customers in meeting IRS 1075 requirements. First, Oracle staff does not have access to customer data or FTI. Next, Oracle staff who support, manage, and monitor OCI US Government cloud regions are US Persons and the data centers are located exclusively within the continental US ensuring data sovereignty. OCI security controls offer customer data isolation and tenant data is always encrypted at rest and in transit.

Cybersecurity Maturity Model Certification (CMMC)

Cybersecurity Maturity Model Certification (CMMC) 2.0 aims to reduce the risks presented by cybercrime, including economic and national security. It implements security controls focused on code, people, and processes. CMMC 2.0 is a new and developing standard that applies to end-user service providers offering goods or services to the US Department of Defense (DoD). CMMC 2.0 is based largely on NIST SP 800-171 and NIST SP 800-172. It unifies the multiple security standards that exist today and offers three levels of certification: 1. Foundational, 2. Advanced, and 3. Expert. CMMC intends to offer reciprocity for CSPs that have achieved FedRAMP.

If you are a CSP customer that is part of the Defense Industrial Base (DIB), your organization must likely comply with the DoD's cybersecurity standards. The original CMMC interim rule went into effect on November 30, 2020, and CMMC 2.0 was released in November of 2021. 3PAOs are currently being accredited and those that achieve accreditation will be authorized to evaluate the CMMC posture of DIBs. DIBs will then be able to select one of the accredited 3PAOs to evaluate the solution built on a CSP to conduct business with the DoD once the CMMC 2.0 policies are finalized.

Demonstrating compliance takes time and effort, so new DoD contracts are unlikely to require CMMC until 2024 when the rulemaking process is expected to be complete. A 3PAO should be engaged for most level 2 assessments to achieve CMMC 2.0 certification. All level 3 achievements undergo government-led triennial assessments. Level 3 is the Expert and highest level with government officials conducting the assessment, and the requirements are still under development. The cost of certification is the responsibility of the organization seeking certification. Customers may achieve Level 1 and some select level 2 through an annual self-assessment.

CMMC 2.0 is not an accreditation that an IaaS or PaaS CSP may achieve because the CSP is not responsible for all the controls that CMMC 2.0 will evaluate. A CSP may assist an end-user in achieving CMMC 2.0 accreditation by offering cloud services with certain demonstrated and proven controls. For example, a cloud provider may achieve FedRAMP High accreditation which certifies controls that CMMC requires. The end-user may use these proven controls, reducing the effort to accredit their overall solution. Also, a company may have multiple CMMC efforts - one to certify themselves as a DIB, and one to ensure their cloud products are aligned with the CMMC controls. These two efforts do not necessarily have any overlap, but both would likely be required of any DIB also acting as a CSP.

Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act (FISMA) requires that all federal agencies follow security standards to safeguard and protect sensitive data. FISMA published a set of data security guidelines based on the controls established by NIST and is designed to protect customer owned on-premises infrastructure. Originally only applicable to federal agencies, FISMA compliance has evolved over time to include state agencies that manage federal programs such as Medicare, Medicaid, and unemployment insurance. FISMA compliance standards are also applicable for vendors and companies that have contracts to work with federal agencies. The prime goals of FISMA are to ensure risk management program implementation, information protection, unauthorized access, destruction, and modification of data, as well as securing the integrity, confidentiality, and availability of sensitive information.

FISMA requirements also include maintaining an inventory of information systems, categorizing information according to risk level, maintaining a system security plan that covers the security controls implemented within the organization and a timetable for the introduction of further controls, conducting continuous monitoring, certification and accreditation, risk assessment, and security controls.

An organization's failure to meet the necessary FISMA requirements or NIST standards may lead to a breach of data, loss of ability to process or handle third-party data, loss of business customers or partners, and regulatory fines.

FISMA impact levels

In cases where a loss of confidentiality, integrity, and availability may occur, organizations should determine the potential impact in accordance with the FISMA compliance levels are either low, moderate, or high impact. FISMA levels are closely aligned with FedRAMP impact levels:

- **Low impact:** Limited adverse effects on organizational operations, assets, or individuals, such as minor damage to organization assets or minor harm to individuals or minimal financial loss.
- **Moderate impact:** Serious adverse effects to organization operations, assets, or individuals, such as significant damage to organizational assets or financial loss or harm to individuals.
- **High impact:** Catastrophic impacts to organization operations, assets, or individuals, such as loss of life or life-threatening injuries to individuals or financial loss or major damage to organizational assets.

FISMA and FedRAMP

FISMA's goal is to protect government assets from unauthorized access and destruction of information and information systems delivered through traditional on-premises deployments. FISMA offers guidelines for government agencies on how to ensure that data is protected. To achieve this goal, FISMA uses NIST SP 800-53A as its primary framework for IT vendors and federal agencies to demonstrate FISMA compliance. FISMA compliant vendors receive authority to operate (ATO) from agencies with whom they do business. FISMA authorization requests are created by the system owner or control provider within the government agency and are granted by the agency's designated authorizing official.

FedRAMP offers guidelines and aims to make the CSP procurement easier on agencies. As FedRAMP inherits the NIST baseline controls, think of it as FISMA for cloud. Because of the overlap between FedRAMP and FISMA security controls, a service or solution that's FedRAMP compliant can be FISMA compliant as well.

Oracle US Government cloud offerings have achieved FedRAMP high JAB P-ATO, joined by the infrastructure and platform services generally available in those regions. Oracle US Government cloud regions may offer an excellent platform to host a service or organization seeking their own FISMA compliance by allowing the agency to inherit applicable OCI FedRAMP controls as they migrate to the cloud.

StateRAMP

StateRAMP is a certification created by a consortium of state governments and CSPs. This authorization is based on the same NIST SP 800 controls that are the basis of FedRAMP. This certification was created to lower the cost, effort, and time barrier that FedRAMP may impose on CSPs, and offers an accreditation option for CSPs who cannot achieve FedRAMP because they do not serve the federal government, and therefore could not get a federal sponsoring agency. StateRAMP is new and is only beginning to see broad adoption by many states and CSPs. StateRAMP has a fast-track program to allow those who have achieved FedRAMP to achieve StateRAMP authorization more quickly.

TX-RAMP

TX-RAMP is a certification developed and managed by the State of Texas. This certification is based on the same NIST SP800 controls that form the basis of FedRAMP. This certification was created to lower the cost, effort, and time barrier that FedRAMP may impose on CSPs, and offers an accreditation option for CSPs who cannot achieve FedRAMP because they do not serve the federal government, and therefore could not get a federal sponsoring agency. TX-RAMP is required of all CSPs offering services to Texas State Agencies and Higher Education institutions beginning on January 1, 2022. Texas is acting as its own accreditation body and will offer reciprocity to CSPs who have FedRAMP or StateRAMP. During the accreditation process, TX-RAMP offers provisional accreditation for 18 months if the CSP offer accreditation evidence for a commercial security standard such as SOC attestations.

Who needs to get accredited?

Who needs to get accredited, and which needed accreditation is driven directly by the customers you wish to serve and the sensitivity of the data that will be processed or stored in the cloud environment. Multiple accreditations may be needed and the larger the customer base you serve, the more accreditations required. If you are a Defense Industrial Base (DIB) and simply want to conduct business with the DoD, you may only need to show adherence to CMMC. If you supply cloud services to the DoD, you will likely need to achieve DISA Impact Level authorization. If you provide cloud services to the federal government, your focus will likely be on FedRAMP. In general, it may make sense to pursue the highest level of accreditation required by your customer base, thus making it easier to show compliance with the other programs, or those targeted at specific workloads like CJIS or IRS1075. Most government accreditations and certification are based on the NIST SP800-53 controls, so the expectations are clear. The main effort will often be determining the impact level (low, moderate, or high) based on the sensitivity of the data processed or stored in the cloud environment.

Security controls

The National Institute of Standards and Technology (NIST) SP 800 controls are designed to help protect sensitive data on non-federal systems. NIST is a unique federal agency with core competency in defining measurement science, devising rigorous traceability, and the development and use of standards. The NIST SP 800 controls form the foundation of most cloud security and stability controls. NIST SP 800 are special guidelines and a subclass of existing computer security requirements for federal data gathered from in the Federal Information Processing Standard (FIPS) 200 as well as the Security and Privacy Controls for Federal Information Systems and Organizations publications. NIST SP 800-53 is specific to federal networks, NIST SP 800-171 are the same controls, but for non-federal networks. NIST SP 800-171 guidelines focus on protecting Controlled Unclassified Information (CUI) in Non-federal Information Systems and Organizations as per their latest publication version (revision 2) released in February 2020.

What is Controlled Unclassified Information (CUI) and what applies?

The National Archives and Records Administration (NARA) administers the program which established the Controlled Unclassified Information (CUI), under Executive Order 13556. It was set in place to tackle several

weaknesses of managing and protecting unclassified information and to standardize the way the executive branch handles such information. Only information that requires safeguarding pursuant to federal law, regulation, or government wide policy may be designated as CUI. The CUI Registry is an online repository for information that requires controls based on government laws and regulations.

Oracle US Government cloud compliance vs customer responsibility
With the implementation of FedRAMP requirements, CSPs demonstrate that in-scope cloud services meet or exceed the requirements of NIST 800-53/171 and customers may inherit certain CSP controls to help meet their own requirements. Customers that migrate their CUI workloads to a FedRAMP accredited cloud have assurance that their cloud-based services and offerings can maintain compliance with US federal security requirements and continue to adapt to the evolving NIST baseline.

Customers may conduct their own FedRAMP and NIST risk-based assessment and rely on the audited controls from 3PAO reports. These reports play a critical role in the security assessment of a cloud service offering, which attest to the effectiveness of the controls the CSP has implemented in its in-scope cloud services.

While some of your controls may be inherited from the CSP, many of the controls are shared between you as a customer, and the CSP. Public sector customers should ensure that their CUI workloads comply with NIST SP 800-51/171 guidelines as well as ensuring compliance with all applicable laws and regulations. It is the customer's responsibility to analyze their cloud strategy to determine suitability of using a CSPs cloud services considering their own regulatory compliance duties.

For more information about NIST 800-171 check out their most recent publication here.

Third-party auditor organization (3PAO)

A key part of achieving authorization or certification is selecting a third-party auditor organization (3PAO). They will be your primary partner when interfacing with authorization bodies. The 3PAO will review your code, your documentation, your process, run scans and penetration tests. They will supply their findings to the authorization body. They may also act as a consultant and supply guidance based upon their experience on how best to achieve controls and maintain compliance. There will be countless decisions that need to be made, each with an associated cost and time requirements. Selecting a 3PAO with experience in your industry may prove beneficial.

For a complete list of FedRAMP authorized 3PAOs, see the FedRAMP website:
https://marketplace.fedramp.gov/#!/assessors?sort=assessorName

Sponsoring agencies

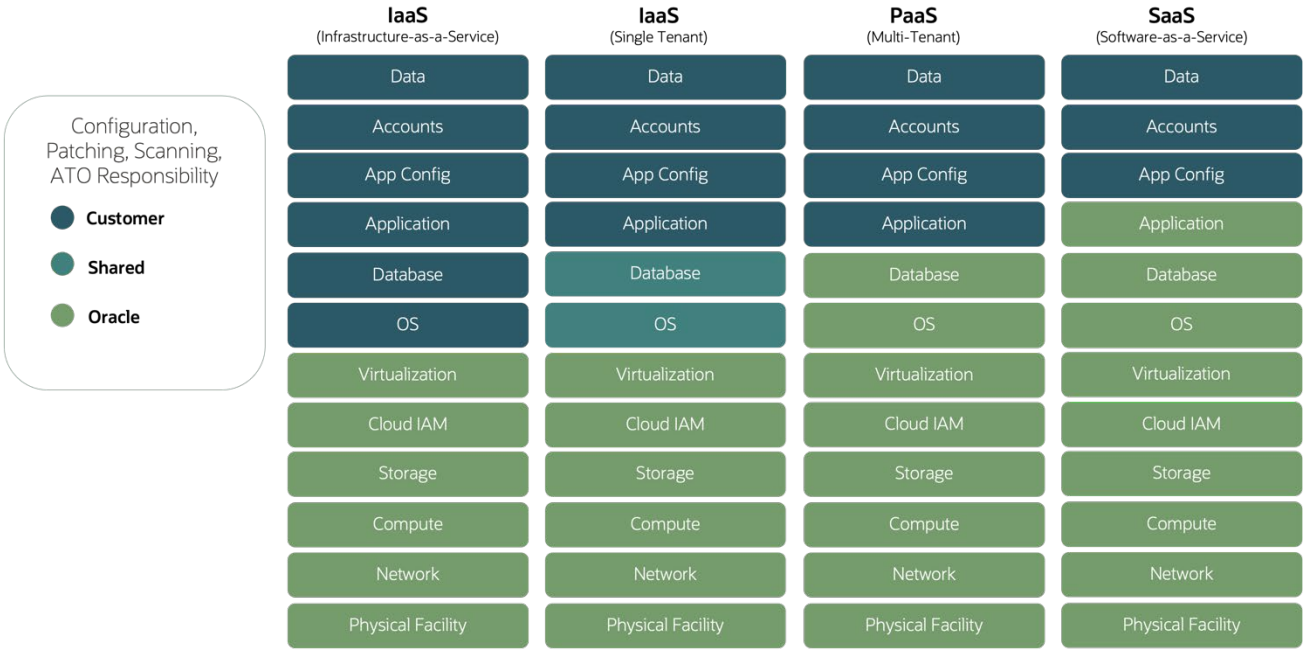
A government sponsor may have to achieve your accreditation (such as FedRAMP or IL). Your sponsor may be an existing customer or a motivated prospect. They may sponsor your accreditation so that they may use your technology to meet their IT strategy goals.

For a full list of agencies who have FedRAMP ATOs: https://marketplace.fedramp.gov/#!/agencies?sort=name

Shared responsibility

Cloud security is a shared responsibility between the CSP and the customer organization running their applications and workloads on the cloud. The requirements that form the basis for FedRAMP, the NIST SP 800-53 controls, detail a set of practices shared between the CSP and the organization consuming the cloud. Some practices are solely the CSP's responsibility and others solely the customer's responsibility. For example, the customer is not involved in the controls associated with physical access to the compute infrastructure, therefore

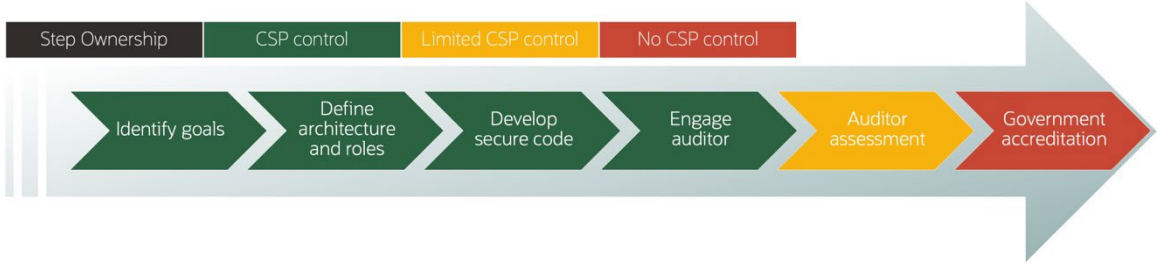
the CSP is responsible for physical security controls. In contrast, the customer handles managing access to their tenancy and cloud resources as the CSP is not responsible for security in the customer's cloud environment/tenancy. Other controls are shared between the customer and the CSP. For example - account management, the CSP supplies the tools to manage the accounts, but it is up to the customer to use them effectively to meet their compliance requirements.



Process and timelines

The time and effort required to achieve DISA or FedRAMP accreditation is extremely variable and program specific. Much of this may be managed with proper planning and guidance. Standardizing your development tools and libraries may help drive the accreditation process more efficiently. If an existing on-premises solution is accredited, the effort to move to the cloud may be much faster and less labor intensive than the original accreditation.

Areas where the CSP may have significant control are in the early stages of the accreditation effort, and these are typically long-standing IT best practices. These include things like starting with a foundation of standard development practices, standardized development tools, clearly defined IT roles, as well as mature upgrade, update, and patching policies. The quality of the documentation you have composed will directly affect how long it takes for the 3PAO to understand your offering and compose a security package.



The FedRAMP website supplies guides and detailed workflows here to give you more information: https://www.fedramp.gov/cloud-service-providers/

Tips

- ✓ Plan and work backwards from target dates - see the FedRAMP website for guidance.
- ✓ Make sure documentation is complete, current, and accessible to those who need it.
- ✓ Contractors may accelerate the timeline in areas where hiring and training are needed.
- ✓ Contractors may cost more over the long run, so plan to hire and/or train personnel eventually.
- ✓ Chose a motivated sponsoring agency. Your sponsor may motivate the accreditation body to move the process faster.
- ✓ Chose a 3PAO who already understands your industry.
- ✓ Design to the highest control standard: have all services meet the highest control standard you plan to achieve.

References

https://www.oracle.com/industries/government/federal/achieving-ato/

https://www.oracle.com/industries/government/govcloud/

https://docs.oracle.com/en-us/iaas/Content/General/Concepts/govoverview.htm

https://www.fedramp.gov/

https://blogs.oracle.com/cloud-infrastructure/post/understanding-and-achieving-fisma-compliance-on-oracle-cloud-for-government

https://blogs.oracle.com/cloud-infrastructure/post/oci-us-government-cloud-and-irs-publication-1075

https://blogs.oracle.com/cloud-infrastructure/post/evolving-compliance-cybersecurity-maturity-model-certification-20-and-the-oracle-government-cloud

https://blogs.oracle.com/cloud-infrastructure/post/oracle-cloud-infrastructure-us-government-cloud-and-itar

Conclusion

Every IT user desires security and availability, and the US Government has made a significant effort to standardize a methodology to achieve this goal. Through the NIST SP800-53 controls and multiple targeted accreditation programs, the government has established a methodology to ensure secure and available cloud-based IT solutions along with a system to demonstrate that security posture to various constituents. While standardization has simplified the process for CSPs and commercial entities needing government accreditation, the process may not be easy. This document highlighted the different accreditation programs and the relationships between them so that you can develop a strategy and approach to determining and achieving your accreditation goals.

The OCI US Government cloud provides a comprehensive suite of tools to enable customers to build a solution in the cloud, from a dedicated SaaS offering to back-office enterprise applications. Based on an entirely generation 2 cloud architecture, with security and auditing built into the foundation of the cloud architecture, customers can be certain to have the tools to deploy a secure, performant, and cost-effective solution that is capable of meeting strict and rigorous government compliance standards. The OCI government cloud offers native and integrated tools to aid in securing a cloud deployment, log and audit tools to capture behaviors, use, and risk, and analytics to understand your control posture.

Acronyms and Terms

3PAO – Third Party Assessment Organization

Accreditation – This term is interchangeable with authorization and certification but may be used to describe the status of a 3PAO, their ability to assess an offering against a standard.

ATO – Authority to Operate

Authorization – This term is often used interchangeably with accreditation and certification but is most accurately used to describe the status of a cloud offering or solution, stating that it has been reviewed against a standard and approved to be used.

Compliant – In the strictest sense this term does not apply to government security standard achievement, it is used to imply that a service or offering meets some grouping of security controls but does not mean it has been reviewed by a 3PAO or an accreditation body.

CJIS – Criminal Justice Information System

CSP – Cloud Service Provider

CUI – Controlled Unclassified Information

CMMC – Cybersecurity Maturity Model Certification

Certified – Often used interchangeably with accreditation and authorization, but is most accurately used to refer to solutions review and approval for TX-RAMP and CMMC, but is not used to describe status for most other security standards

DIB – Defense Industrial Base

DISA – Defense Information Systems Agency

FedRAMP – Federal Risk and Authorization Management Program

FISMA – Federal Information Security Modernization Act

FTI – Federal Tax Information

IaaS – Information as a Service

IL – Impact Level

IRS1075 – Internal Revenue Service publication 1075

ITAR – International Traffic in Arms Regulations

JAB – Joint Authorization Board
NIST – National Institute of Standards and Technology

PA – Provisional Authorization

PaaS – Platform as a Service

SaaS - Software as a Service

SRG- Security Requirements Guide

StateRAMP – State Risk and Authorization Management Program

TX-RAMP – Texas Risk and Authorization Management Program

USML – United States Munitions List

Connect with us blogs.oracle.com facebook.com/oracle twitter.com/oracle

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