ORACLE

Oracle Cloud Infrastructure Sovereign Cloud Principles

Considerations for Implementing Cloud Data Sovereignty Strategies in a Complex and Fast-Changing Regulatory Environment

February, 2024, Version 1.0

Public

ORACLE

Purpose Statement

This document provides an overview of some, but not all, features and enhancements that may be considered for cloud sovereignty strategies and deployments. It is intended solely to help customers assess the business benefits of necessary planning for the implementation of sovereign cloud deployment strategies and product features associated with those possible strategies.

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license 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 in planning for the implementation and upgrade of the product features described. 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 in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

ORACLE

Table of Contents

ORACLE

About Oracle Cloud Infrastructure

Oracle Cloud Infrastructure (OCI) is a cloud platform designed to help customers modernize, adapt, and innovate. With OCI, customers can migrate, build, and run all their IT, from existing enterprise workloads to new cloud native applications and data platforms.

OCI's distributed cloud provides customers with the flexibility to choose where and how cloud services are delivered to meet their regulatory, performance, and other needs. OCI's distributed cloud offerings deliver the full functionality and superior economics of Oracle's public cloud to customer data centers and edge locations, with a range of deployment models and operational controls.

Oracle's Approach to Data Sovereignty

Data sovereignty is a complex topic, and the definition and applicability can vary by region. However, a central theme of data sovereignty is empowering organizations and individuals to retain more control over their data. Though often discussed as a singular item, data sovereignty comprises different parts.

When defining a cloud data sovereignty strategy, consider the following factors:

- **Choice of location:** The physical location where the data is stored
- **Cloud isolation:** Physical, logical, and network separation to limit sharing of data
- **Access management:** Customer control over their data and the underlying infrastructure, both by limiting access and ensuring data availability and portability for those they authorize
- **Operations personnel requirements:** Restriction of operations and support to personnel meeting specific security clearance, citizenship, or residency requirements
- **Enhanced hardware and software security:** Use of capabilities, such as confidential computing, hardware security modules (HSM), and external key management
- **Transparency in data access decisions**: Handling and reporting on extraterritorial law enforcement requests for data access, including interactions with local authorities

Principle 1: Location

An organization should have the ability to choose the geographic regions where it stores its data.

Data Location and Its Impact on Data Sovereignty

Consider the following factors in determining the appropriate cloud deployment model for your organization's objectives:

- **Data classification:** The type of data that the organization plans to store in the cloud based on its business standards and any applicable regulations
- **Data storage:** Restrictions and data protection regulations provide requirements for sensitive data that might need to be stored within the geographic boundaries of a country or region
- **Data availability:** Uninterrupted access to data and services vital to business operations, government functions, or public infrastructure security

The choice of location for data can help organizations meet their data storage and availability needs in line with data processing and data transfer requirements under applicable data protection laws.

OCI Deployment Models

OCI offers several deployment models to help organizations with their data sovereignty strategy. OCI segments these deployment models into public cloud offerings, operating out of Oracle's cloud regions and dedicated cloud offerings deployed in a customer's data center. Each deployment option allows Oracle customers to maintain control of their data, including the location of the region where it has been stored and processed and how it's accessed. Customers remain in control of their data, and Oracle doesn't move customer data out of the region where it resides without customers' authorization.

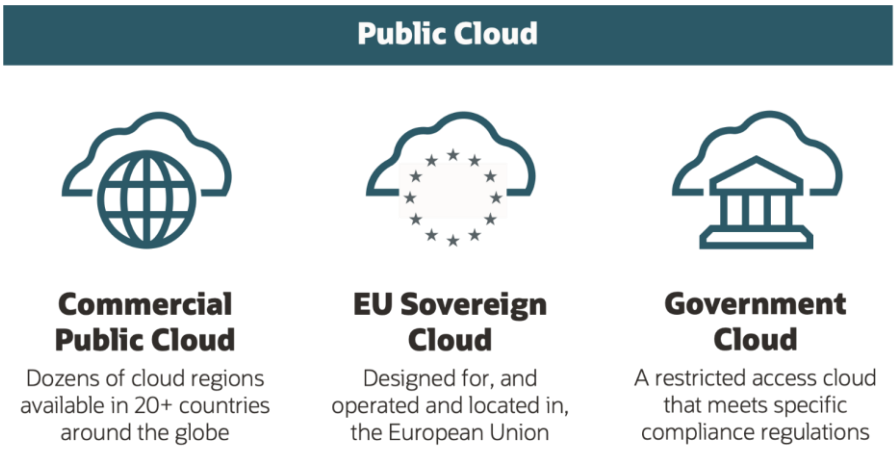

Figure 1. OCI Public Cloud Offerings

Oracle offers the following public cloud options:

- **Oracle commercial public cloud**: Offers dozens of cloud regions in over 20 countries, with more to come. In more than 10 countries and across the EU, OCI has two or more cloud regions that enable availability in the event of a disaster without data leaving the borders of these territories. Many organizations operating in these locations can run cloud workloads in-country to meet their data residency and availability requirements. Each OCI region offers a consistent set of more than 100 cloud services designed to run any application faster and more securely for less.
- **Oracle EU Sovereign Cloud**: Oracle's EU Sovereign Cloud regions are logically and physically separate from the existing Oracle commercial cloud regions in the EU. Both private companies and public sector organizations can use these new EU Sovereign Cloud regions to host data and applications that are regulated or of strategic regional importance.
- **Government cloud**: Offers cloud regions in the United States, United Kingdom, and Australia, which are restricted to their respective government communities.

Organizations can use the following examples of Oracle's dedicated cloud solutions to host complete cloud regions on-premises in a data center of their choice. These options can help organizations in geographies where Oracle doesn't yet offer a public cloud region or if the organization has unique data sovereignty requirements that need a dedicated solution.

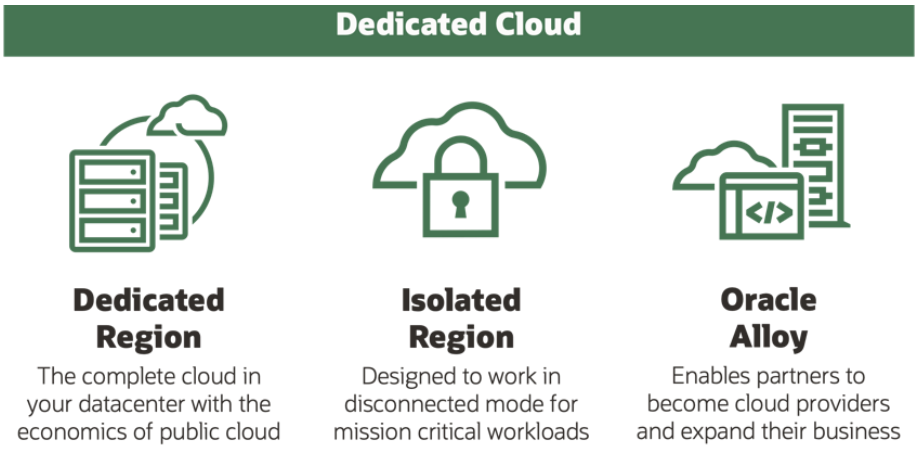

Figure 2. OCI Dedicated Cloud Offerings

Oracle offers the following dedicated cloud options:

- **OCI Dedicated Region:** Designed for organizations looking for a complete OCI region in their data center with the agility, scalability, and economics of the OCI commercial public cloud
- **Oracle Cloud Isolated Region:** Designed for organizations who need a proven cloud platform for their classified, top secret, mission-critical workloads
- **Oracle Alloy:** Enables partners looking to become cloud service providers with a full range of cloud services to expand their business

Oracle aims to meet organizations where they are, both literally and figuratively. For many organizations, Oracle customers find that Oracle's commercial public cloud regions are more than sufficient to meet their data sovereignty needs, including the need to choose where data is located. However, for highly regulated industries or organizations subject to certain country-specific legislation, the enhanced data sovereignty options from Oracle EU Sovereign Cloud, government cloud, or one of the dedicated cloud solutions can accelerate OCI customers' cloud-first strategy.

Principle 2: Isolation

An organization should have the assurance that their data remains in the physical and logical environments that they have selected.

Using Realms for Enhanced Isolation

OCI provides this technical assurance by grouping regions and then separating these groups of regions through strict geographic segmentation and physical and logical network isolation. This separation allows OCI to implement different operational processes, further enhancing customers' ability to maintain sovereignty over their data. At OCI, these separated groupings of cloud regions are called realms.

A realm is a logical collection of cloud regions that are isolated from each other and don't allow customer content to traverse realm boundaries to a region outside that realm. Each realm is accessed separately. OCI has multiple realms, including a commercial public cloud realm, an EU Sovereign Cloud realm, and multiple government cloud realms for the US, UK, and Australia. Each customer's Dedicated Region, Isolated Region, and Alloy deployment are also contained within their own separate realm.

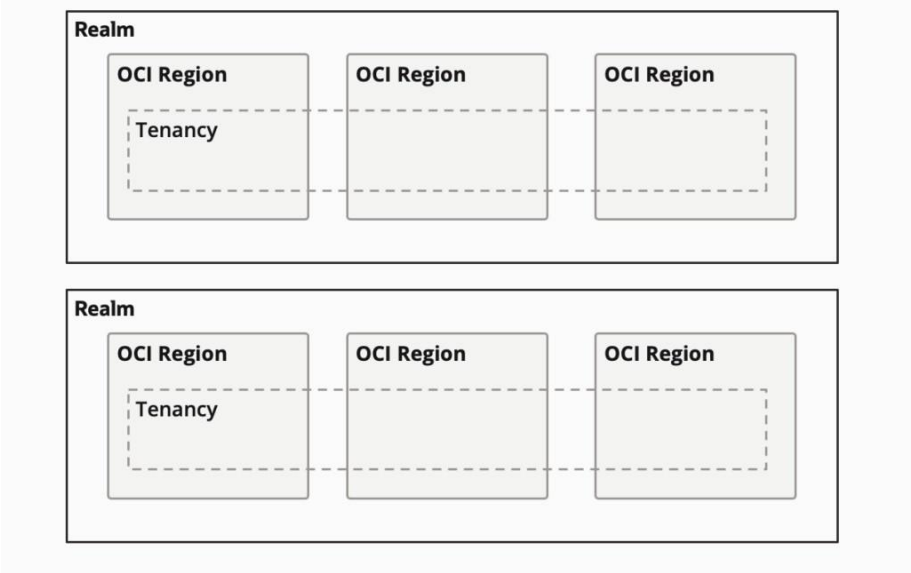

Figure 3. OCI Realm Isolation

A realm enables Oracle to provide defined capabilities across regions that are designed to meet the specific regulatory requirements of different customer types. OCI's unique isolated realm architecture simplifies and strengthens data sovereignty and controls, whereas other cloud providers might rely on customer-controlled policies or confidential computing. While OCI also offers these features, it simplifies sovereign cloud governance with operations, support, and policies that can be distinct from Oracle's commercial public operations.

Realms Support Sovereignty Requirements

Customers access cloud resources and services through their cloud tenancy. A cloud tenancy is a secure and isolated partition of OCI, and it only exists in a single realm. Within this tenancy, customers can access services and deploy workloads across all regions within that realm by default, although customers can set policies to restrict this access. However, by design, customers can only access regions within the realm of their tenancy. For example, if a customer has a tenancy in OCI's commercial public cloud realm, the customer can run workloads in any of the commercial regions. However, a customer can't access OCI's EU Sovereign Cloud regions because they're in a separate realm. This design ensures that hosted data remains within the cloud regions of a realm by default and can't be moved to a different region outside of that specific realm. OCI has applied this same methodology across public and dedicated cloud realms.

EU Sovereign Cloud Realm and Its Benefits

Customers, such as a government agency or EU member state government, can expect multiple technical benefits when running their workloads in the EU Sovereign Cloud realm. One common risk that blocks EU member states from migrating workloads to the public cloud is losing control of their data locality. EU organizations might be concerned with data flowing out of the EU or being replicated to a physical resource, such as a server or a backup drive located outside the EU, and the potential implications of extraterritorial laws, such as the US CLOUD Act.

EU organizations using the Oracle EU Sovereign Cloud realm benefit from a unique architecture that provides a clear, simple separation of operations from commercial regions to help meet heightened compliance requirements. A low-latency network between data center locations allows applications to span multiple geographies and offers resilience for disaster recovery, while still maintaining hosted data within the boundaries of the EU.

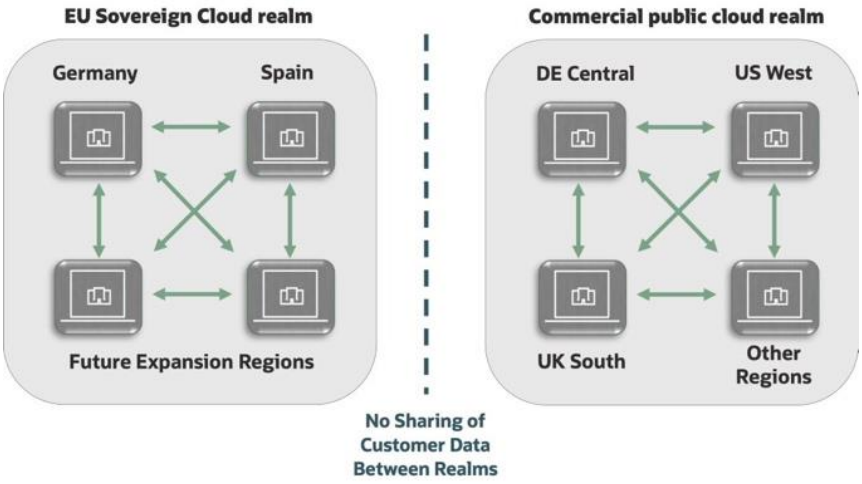

Figure 4. OCI EU Sovereign Cloud Is Isolated from Commercial Public Cloud Realm

As depicted in Figure 4, the data flow (identified by green arrows) doesn't extend beyond the logical confines of the realm itself and is limited to within the realm. The isolation of the EU Sovereign Cloud realm from the commercial public cloud realm allows Oracle to restrict support and operations personnel to EU residents, including physical and logical access to the realm. The hardware and assets used to provide these cloud regions are owned, operated, and managed by EU legal entities that are separate from the existing global Oracle entities, including those in the EU. This design provides added assurance that all aspects of managing and hosting data in the EU Sovereign Cloud stay within the EU. Customers can choose to run in a specific single region of the EU Sovereign Cloud realm or run in both regions, depending on a customer's business requirements.

Principle 3: Access Management

An organization should have the option to limit access to the data they store in the cloud and ensure the availability and portability of that data.

How Oracle Manages Access to OCI

Oracle manages its engineering and operations teams' access to the parts of OCI that are necessary to develop, administer, and support OCI. Access to OCI is based upon the concept of least privilege, which means restricting role entitlements to the minimum required to perform functions and implementing strict identity authorization policies. Access of operations staff to the infrastructure and services supporting OCI requires multifactor authentication (MFA), a VPN connection, and an SSH connection with a user account and password or private key.

Security doesn't end with authorization and authentication. Monitoring access is just as critical. OCI employs solutions to continuously monitor authentication logs for servers and network devices supporting OCI services.

The same access controls are implemented across all OCI deployment models. However, sometimes, the ability to manage access requires the ability to implement more layers of restrictions based on the security clearance and residency of personnel. Thanks to this realm isolation, Oracle has engineered a process to support this type of enhanced access restriction. These added levels of access control stand at the core of OCI's distributed cloud strategy and allow OCI to offer distinct support and operations models for its Government Cloud regions, Isolated Regions, and EU Sovereign Cloud regions.

How Customers Manage Access in OCI

As a cloud provider, Oracle has no insight into the customer data that customers collect, process, or store in OCI. Customers are responsible for the security of their data in the cloud, and part of implementing good security practices includes managing access to cloud resources and data, including properly classifying data and meeting any associated compliance requirements. In data sovereignty, this aspect includes protecting against unauthorized access, use, or disclosure of data.

Regardless of which cloud deployment model a customer selects, OCI's services and capabilities provide features that can limit access to cloud resources and data stored in customer cloud tenancy and help monitor access and security risks. Organizations can use the following core OCI services to implement a comprehensive approach to access management:

- The **Identity and Access Management (IAM)** service lets customers control who has access to their organization's cloud resources. IAM is flexible enough to support customer security models across tenancies or be restricted to a single tenancy, compartment, or set of resources.
- **Vault Key Management** provides centralized management of the encryption of customer data with keys that a customer can control. Create, rotate, enable, or disable keys, assign keys to resources, and use keys for encryption and decryption to safeguard data. Customers can implement Vault either as a multitenant software-based key management service or as a dedicated HSM module, as the situation dictates. In either case, Vault is exclusively located within the realm.
- The **Audit** service logs calls to the OCI public application program interface (API), whether those calls originate from the Oracle Cloud Console, software developer kit (SDK), or command line interface (CLI). Audit log contents include the activity that occurred, the user who initiated it, the date and time of the request, the source IP address, the user agent, and more. Data from these logged events can help customers safeguard their data by enabling them to monitor the activity within their tenancy, including tracking administrative actions on their keys and vaults.
- **Access Governance** is a cloud native identity governance and administration (IGA) solution that delivers insights-based access reviews, identity analytics, and intelligence capabilities. It enables customers to audit user capabilities and actions to determine current appropriate levels of access to tenancy administration functions.
- **Cloud Guard** and **Security Zones** work together to define and enforce security policies for a customer's configuration and users, monitor changes and activity in their tenancy, and take corrective actions when issues are detected.

OCI Offers Portability and Availability of Data to Customers

As more customers adopt a multicloud approach, Oracle recognizes the importance of data portability and availability. Organizations' ability to control their data, including the ability to switch cloud providers, is an essential aspect of data sovereignty. Oracle makes it easy and cost-effective for customers to move their data in and out of OCI, even for workloads with massive data migration requirements.

Oracle believes that if customers need to migrate their data, they shouldn't be penalized for it. Unlike other cloud service providers that restrict customer data with high pricing for network egress, OCI's approach gives customers everyday low pricing for network egress and free ingress. Oracle also makes contractual commitments to ensure that customer data rights remain intact, even in the event of termination and exit.

Principle 4: Personnel Requirements

An organization should have the ability to restrict the types of individuals working on their cloud environment, based on residency, security clearance, and so on.

Differences Between Operations and Support

Cloud operations provides continuous monitoring of performance and proactively addresses security issues through tactics like logging and patching. For example, one of the teams part of OCI cloud operations is the OCI Security Operations team, which is responsible for monitoring and securing the OCI hosting and virtual networking technologies. This team works directly with OCI Engineering to remediate security-related issues. The team monitors emerging internet security threats and implements appropriate response and defense plans to address risks to OCI and its customers. When the security operations team responds to a security threat, they act according to documented processes, and all actions are logged in a secure ticketing system. They apply a high standard of care to protect service and data integrity, privacy, and business continuity.

Cloud support ensures that customers can rely on OCI for consistent availability, performance, and management of cloud resources. Based on industry-leading service level agreements (SLAs), Oracle delivers the support and engineering services needed to resolve any issues that prevent consistent performance or customers' ability to manage, monitor, or modify their cloud resources. The most visible part of this group provides OCI tenants with 24/7 support through the My Oracle Support ticket management application and the skilled personnel needed to triage and resolve support requests in alignment with SLA commitments. Unlike other cloud providers, this level of customer support comes at no extra cost to customers using OCI services.

OCI's Operations and Support Models

OCI operations and support models vary between distributed cloud deployment offerings. Oracle's realm isolation allows customers to offer role-based personnel services based on their use case and regulatory requirements.

Selecting the appropriate operations and support model depends on customer requirements and the needs of the organization. OCI offers a global team consisting of highly trained cloud engineers that provide 24/7 operations and support to commercial public and dedicated cloud regions. For most cloud customers, this global team is more than sufficient to meet their business objectives.

However, Oracle recognizes that many organizations have unique data sovereignty requirements that might require more restrictions when it comes to who provides cloud operations and support and where they're physically located. For example, some regulators in the EU are focusing on data sovereignty and cross-border data transfer issues, which impacts how support is provided, particularly for sensitive workloads.

Oracle EU Sovereign Cloud

Oracle EU Sovereign Cloud offers cloud regions that are located exclusively within the geographic boundaries of the EU. Both commercial and public sector organizations can use these regions to host their cloud applications and customer data within the EU to meet data protection and sovereignty requirements.

EU Sovereign Cloud operations and support personnel have completed identical training and skills curriculum as OCI's global operations and support team and have the following attributes:

- **EU residency:** Personnel that provide customer support, data center support, and data center operations for EU Sovereign Cloud are required to be EU residents.
- **Employed by separate legal entities**: Personnel are employed by Oracle EU Sovereign Cloud entities located throughout the EU that are responsible for customer support, data center support, and data center operations needed to support the EU Sovereign Cloud data regions.

- **Separate support request system:** Personnel provide customer support for issues, such as troubleshooting, password reset, and ticket management. This ticketing system is contained within the EU Sovereign Cloud realm and separate from other OCI realms.

EU data residency combined with realm isolation and local support and operations provides customers with enhanced separation from OCI's other public commercial cloud regions and increased protection from extraterritorial law enforcement requests.

Oracle Cloud for Government

Oracle Cloud for Government is a cloud deployment model providing the full OCI service portfolio, designed to comply with the specific security, compliance, and sovereignty requirements of national governments. OCI operates cloud regions for the US, UK, and Australian governments.

Government region cloud operations and support personnel have completed identical training and skills curriculum as OCI's global operations and support team and have the following attributes:

- **Residency:** Personnel must comply with residency requirements set by the government.
- **Security clearance:** Personnel might need to hold specific security clearance requirements, such as SC Level Security Clearance in Oracle Cloud's UK government regions.
- **Separate support request system**: Local security-cleared personnel provide customer support for issues, such as troubleshooting, password reset, and ticket management. This system is separate from other OCI realms.

These restrictions offer government and public sector organizations added trust in the individuals who are providing support and operations.

Oracle Cloud Isolated Region

Oracle Cloud Isolated Region is a secure, air-gapped OCI solution designed to meet the highest demands of global customers' mission-critical classified workloads. Isolated Regions deliver compute, security, storage, and networking services in an on-premises environment, which is disconnected from the internet at the location of the customer's choosing. These regions offer the same services as public Oracle Cloud Regions. Dedicated to serving governments and safeguarding global defense missions at hyperscale, this innovative cloud solution includes a fully integrated infrastructure with infrastructure, platform, and software as a service (IaaS, PaaS, and SaaS).

Isolated Region operations and support personnel have completed identical training and skills curriculum as OCI's global operations and support team, plus more training to function within a government's classified and air-gapped environment. Unique differences with the Isolated Region support model include the following examples:

- **In-country residency**: Personnel are physically located within the country in which the region is located.
- **Citizenship:** Personnel are citizens of the customer's respective country.
- **Security clearances**: Personnel might be required to maintain the customer-defined security clearance level.
- **Dedicated team**: Personnel provide dedicated support and operations for a single customer.
- **Separate support request system**: Local security-cleared personnel provide customer support for issues such as troubleshooting, password reset, and ticket management. This system is separate from other OCI realms.
- **Joint operations**: The customer can provide staffing for joint operations for all roles in the country in which the region is located.

Isolated Regions offer government organizations OCI's highest level of control for their operations and support model. This approach is designed to ensure that a government's most critical and classified data is safeguarded, SLAs are achieved, and the customer is always mission-ready.

Principle 5: Encryption

Organizations should have access to cryptographic solutions that are designed to maintain confidentiality, integrity, availability, and control access to data.

Confidential Computing

A confidential instance is a Compute virtual machine (VM) or bare metal instance where both the data and the application processing the data are encrypted and isolated while the application processes the data, preventing unauthorized access or modification of either the data or the application. Currently, OCI offers confidential computing on bare metal and VMs that use AMD EPYC processors.

Confidential computing has several benefits for organizations to consider as they decide how to augment their security posture to include confidential computing VMs or bare metal servers. By providing security through foundational layers of hardware, confidential computing minimizes the list of trusted parties, including OS, ecosystem partners, and administrators, reducing the risk of data exposure. By providing a smaller attack surface and more security of data in use through a tightened hardware-based root of trust, it protects against some types of vulnerabilities, such as insider threats and firmware compromises.

Confidential computing has the following main benefits:

- Improved isolation using real-time encryption
- Data and applications are encrypted using a key unique to the VM that isn't accessible from any applications, VM or instance, the hypervisor, or to OCI.
- No change is required to the application to enable confidential VMs.
- Protects data in-use with minimal performance impact to the applications
- Customers can implement with no extra cost on top of OCI Compute instance pricing.

In highly regulated industries, such as finance, healthcare, and defense, protecting data throughout its entire life cycle is critical. Using confidential computing to encrypt and isolate data in use on OCI Compute instances can help customers to meet and maintain regulatory compliance and support sovereign cloud strategies.

Vaults

Vaults are logical entities that create and securely store keys and secrets, such as passwords, certificates, SSH keys, or authentication tokens. Oracle's key management service, OCI Vault, currently offers two vault types to accommodate an organization's needs and budget. The type of vault a customer selects determines the features and functionality, such as the degree of key storage isolation, access to management and encryption, scalability, backups, and pricing. Both options store customers' keys on an HSM, but customers can use either a dedicated or multitenant HSM partition.

A dedicated partition houses virtual private vaults, which offer more isolation, backup and restore, and cross-region replication. Virtual private vaults include 1,000 key versions by default. If a customer doesn't require this degree of isolation or the ability to back up the vault, they don't need a virtual private vault. Without a virtual private vault, customers can help manage costs by paying for key versions individually as they need them.

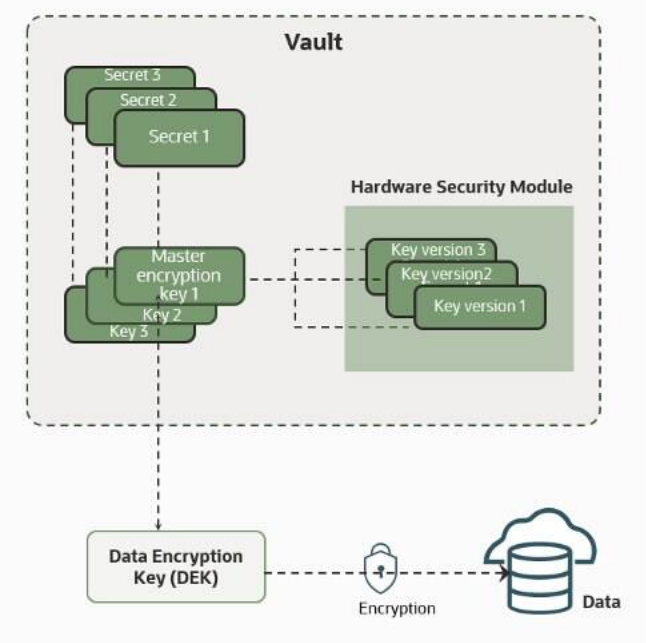

Figure 5. OCI Key Vault for Hardware Security Modules

Hardware Security Modules

An HSM is designed to provide dedicated cryptographic functionality, including key generation, key storage, and digital signing, on a one-to-one basis to their host applications. HSMs are specialized hardware that's harder to access than normal server memory, making them part of a traditional security best practice design. OCI Vault uses HSMs that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification. This certification means that the HSM hardware is tamper-evident, has physical safeguards for tamper-resistance, requires identity-based authentication, and deletes keys from the device when it detects tampering.

OCI Vault can use HSMs to generate and store a root of trust (RoT) that protects encryption keys used by OCI Vault to safeguard users' keys and credentials. When using OCI Vault service with an HSM, keys and credentials can be read if the RoT stored in the HSM is available. Because HSMs are designed to make the RoT difficult to extract, this system significantly mitigates the risk of compromise of users' keys and credentials.

By using OCI Vault and HSMs, OCI customers can benefit from the following features:

- **Secure key management:** OCI Vault provides a centralized and secure approach to key management. Keys are crucial components in cryptographic systems, and their protection is vital to ensure the confidentiality, integrity, and availability of data. OCI Vault and HSM can help organizations generate, store, protect, and manage cryptographic keys throughout their lifecycle, including key generation, distribution, rotation, revocation, and destruction. Customers can also use their own security keys hosted on the HSM to encrypt their data.
- **Compliance and regulatory requirements:** Many industries and jurisdictions have specific compliance and regulatory requirements for protecting personal and sensitive data. OCI Vault and HSM solutions enable organizations to meet these requirements by providing a robust framework for encryption and key management. Compliance frameworks, such as the Payment Card Industry Data Security Standard (PCI DSS) and guidance issued under the General Data Protection Regulation (GDPR), require the use of secure key management practices.

- **Data integrity:** OCI Vault and HSM play a crucial role in ensuring the confidentiality and integrity of data. By securely managing cryptographic keys, organizations can encrypt sensitive information and protect it from unauthorized access or tampering. OCI Vault can help enforce strong encryption practices and enable organizations to maintain control over their data, even if when it's stored or processed by third-party services or cloud providers.
- **Enhanced security for applications and systems:** OCI Vault and HSM offer a higher level of security for applications and systems that require cryptographic operations. By migrating key management and cryptographic operations to dedicated hardware or secure services, organizations can benefit from the robust security features provided by OCI Vault, including protection against attacks, such as key theft, tampering, or unauthorized usage.
- **Protection against insider threats:** OCI Vault and HSM can help mitigate risks associated with insider threats. With proper access controls and separation of duties, organizations can limit the exposure of cryptographic keys to authorized personnel only. OCI Vault and HSM provide audit logs and monitoring capabilities, allowing organizations to track and detect any unauthorized or suspicious activities related to key management.
- **Trust and assurance:** Utilizing OCI Vault and HSM can enhance trust and assurance in the security of an organization's cryptographic operations. By adopting industry-standard practices and technologies, organizations demonstrate their commitment to protecting sensitive information. This aspect can be particularly important for businesses that handle sensitive customer data because it helps build trust with customers, partners, and stakeholders.

OCI Vault and HSMs are available in all OCI's distributed cloud deployment models and provide centralized management of the encryption of customer data with keys that the customer controls.

OCI External Key Management Service (KMS)

Built in partnership with the Thales Group, OCI External KMS enables organizations to store their OCI keys externally on virtual or physical Thales CipherTrust Cloud Key Manager (CCKM) appliances. Using Thales CCKM, organizations can store their keys in a FIPS 140-2 Level 3 appliance and have the flexibility to choose the location of their encryption keys and to ensure data can't be read outside of certain national boundaries. This function includes the capability to store and manage cloud and on-premises keys with the same CCKM appliance for a seamless experience for existing Thales customers.

External KMS uses Thales' Hold Your Own Key (HYOK) functionality and enables customers to encrypt their data using encryption keys that the customer creates and manages outside of their OCI tenancy. External KMS encryption keys always stay within the custody of the customer and are never imported into OCI, putting customers in control of the physical storage of keys outside the cloud. This service helps OCI customers address their data protection and regulatory requirements and be assured that Oracle operators never manage their keys.

Using External KMS also provides an extra level of protection by disabling master encryption keys from customers' own key management system, and if a security incident occurs, data in the cloud is prevented from being decrypted. Regardless of which OCI deployment model customers choose, whether OCI's public cloud, Oracle EU Sovereign Cloud, or an OCI Dedicated Region, they can access all of the same key management features.

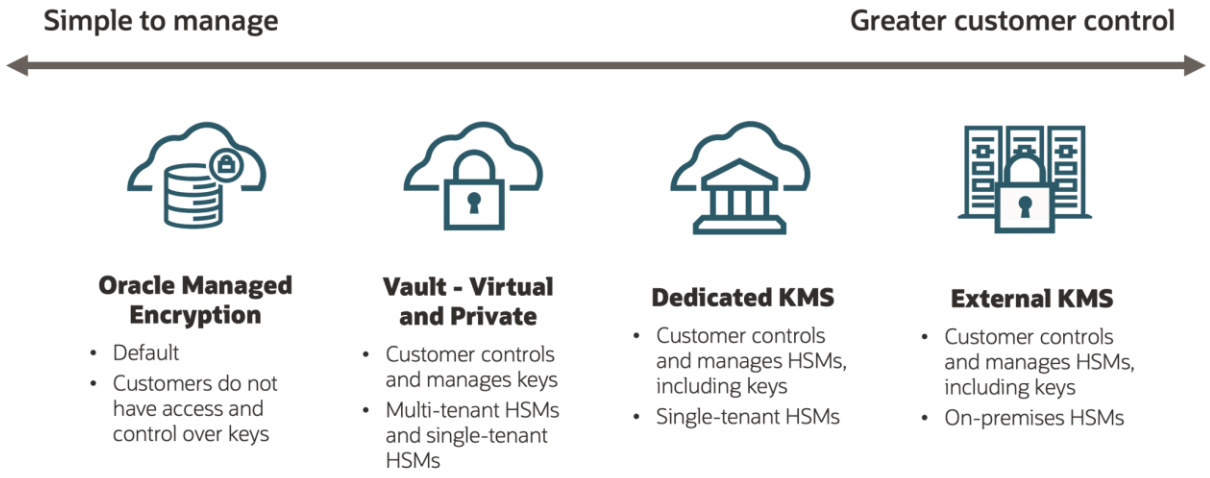

Figure 6. OCI's Key Management Offerings

Combining External KMS with Oracle EU Sovereign Cloud

Complementing EU Sovereign Cloud with the External KMS feature on Thales CCKM provides customers with more security control capabilities to strengthen their sovereignty strategy. External KMS allows segregation of duty between the key management and custody solution and the encrypted resources in OCI. By using solutions from Thales, an EU company with Common Criteria certified HSM solutions, customer ownership, and control of encryption always keeps customers in control of their data encryption.

Principle 6: Data Access Requests

An organization should have visibility into how their cloud provider evaluates and responds to law enforcement requests in relation to their data.

Other Sovereignty Safeguards for Customer Data

To provide customers with reassurances regarding data access requests, Oracle has taken an approach with the following steps:

- **Sovereignty by design:** Developing products and solutions that provide enhanced sovereignty capabilities
- **Legal access request evaluation:** Assessing how to handle information requests submitted by law enforcement agencies and governments
- **Transparent reporting:** Offering publicly available reports on interactions with law enforcement
- **Ongoing regulatory engagement:** Staying abreast of legislation through regular discussions with lawmakers and regulators

This approach is intended to provide customers with both enhanced control over their data and transparency about how Oracle handles access requests.

Evaluation of Legal Access Requests

Customers typically have direct access to the data stored in their tenancy. So, Oracle believes that customers are generally in a better position to identify and access their own data in response to a legal access request.

If Oracle receives a disclosure request directly from a law enforcement or government authority, the Data Processing Agreement for Oracle Services and Oracle's Binding Corporate Rules (BCR-p) provide for the following safeguards:

- Oracle challenges any access request that isn't binding and valid under applicable law. Some statutes, such as the US CLOUD Act, provide multiple avenues for services providers to challenge access requests.
- Oracle promptly notifies the customer, including the customer's and Oracle's data protection authorities, without otherwise responding to the access request, subject to the following terms:
    - If Oracle is expressly prohibited under applicable law from informing the customer, such as preserving the confidentiality of a criminal investigation, Oracle requests that the authority who made the request waive this nondisclosure prohibition. Oracle documents that it has requested this waiver.
    - Oracle requests that the authority that made the request extend the response deadline to enable the customer's and Oracle's data protection authorities to take a view on the validity of the request.
    - Oracle provides the minimum amount of information permissible when responding to a legal access request based on a reasonable interpretation of the request.

For EU Sovereign Cloud, Oracle has EU legal teams responsible for evaluating each legal access request on a case-by-case basis to determine whether the disclosure request is binding and valid under applicable law.

By design, Oracle built the EU Sovereign Cloud using separate EU legal entities. This structure offers more protection from non-EU data access requests. Oracle's view is that the safeguards offered by the EU Sovereign Cloud realm, such as isolation, local support and operations, and Oracle's process for handling data access requests supports Oracle's position that an Oracle entity receiving a data access request under the US CLOUD Act shouldn't have possession, custody, or control of EU Sovereign Cloud tenant data.

EU Sovereign Cloud Governance Committee

With the EU's rapidly evolving regulatory landscape, OCI's EU Sovereign Cloud regions have a specific EU Sovereign Cloud Governance Committee dedicated to monitoring regulatory changes and evaluating how they might impact EU Sovereign Cloud customers. Comprised of senior EU-based employees with expertise in security, data protection, and cloud operations, the Governance Committee is chartered with ensuring that OCI is addressing the needs of EU Sovereign Cloud customers across all aspects of the product, from supply chain to HR policies. Collectively, they help ensure operational integrity and perform periodic reviews to ensure the overall effectiveness of controls and commitments.

Offering Transparent and Publicly Available Reporting

Oracle publishes a report every six months to provide customers with information about the requests submitted to Oracle by law enforcement agencies and governments from around the world. These law enforcement request reports are available on Oracle's website and provide insight into the type of requests received and if Oracle provided a response.

Oracle also publishes privacy policies and cloud service contracts online, which include clear purpose-limitation restrictions for the use of customers' personal information and safeguards around legally required disclosure requests from law enforcement.

Bringing Thought Leadership to the Regulatory Landscape

Oracle proactively engages with global regulators to ensure that OCI supports its customers' data protection and sovereignty requirements. For example, Oracle has been closely monitoring the European Cybersecurity Certification Scheme for Cloud Services (EUCS) and other emerging cloud security frameworks to ensure that OCI continues to develop products that meet market demands.

ORACLE

One Cloud Does Not Fit All

Oracle firmly believes that cloud computing is no longer a one-size-fits-all. Organizations' needs vary depending on the region they're located in, the industry they operate in, and the kind of data they are managing. Though a market for services operating in massive hyperscale public clouds continues to exist, organizations with key sensitive workloads increasingly demand reliable, secure cloud services that run from a more diverse set of footprints.

Oracle is committed to helping customers operate in a fast-changing global economy and complex regulatory environment by providing organizations with the technology and flexibility they need. This assistance includes an ongoing effort to design cloud capabilities that help customers meet data protection regulations and secure their most sensitive citizen, government, or other data.

For questions about Oracle sovereign cloud solutions, contact one of OCI's representatives. To learn more about Oracle Cloud Infrastructure's distributed cloud deployment offerings, see the following resources:

- Oracle Public Cloud Regions
- Oracle EU Sovereign Cloud
- OCI Dedicated Region
- Oracle Cloud Isolated Region
- Oracle Alloy

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