CMMC Level 3 Informational Guide

Guidance to achieve CMMC Level 3 compliance with Oracle Cloud Infrastructure

DecemberDecember, 2025, Version [1.0]

Public

Purpose statement

This document is designed to provide basic guidance to the Defense Industrial Base community who need to achieve Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 3 compliance.

Disclaimer

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. It does not constitute a contract or amend or expand any services term in Your order for Oracle Cloud Services. The development, release, and timing of any features or functionality described in this document—and changes thereto—remain at the sole discretion of Oracle.

Some of the services are under specific accreditation by the US Government and may not be available as a general release.

Oracle's CMMC 2.0 guidance is based on U.S. Department of Defense (DoD) information, found at https://dodcio.defense.gov/CMMC/, current as of October 2024. The CMMC 2.0 Program rule 32 CFR was published October 15, 2024. The CMMC 2.0 program requirements and DFARS implementation are currently under rulemaking processes.

Information in this document is subject to change. Please check the DoD's CMMC 2.0 guidance and the Federal Register for the latest information.

Table of contents

Introduction

This basic guide is designed to assist the Defense Industrial Base (DIBs) that will pursue CMMC Level 3 certification. CMMC Level 3 is additive to CMMC Level 2, therefore, this guide is specific to Level 3 and assumes you have reviewed the CMMC Level 2 guide to meet those pre-requisites. Your government contracts/subcontracts will dictate your applicable level of CMMC compliance. CMMC Level 2 expands to 110 controls, and Level 3 requires all 110 controls in addition to 24 NIST 800-172 controls. Oracle US Government Cloud has achieved FedRAMP High P-ATO, which means that Oracle Cloud Infrastructure (OCI) services running within Oracle US Government Cloud data regions meet applicable NIST 800-171 and applicable NIST 800-172 control requirements (these are all included in the superset of NIST 800-53). All OCI references are to the Oracle US Government Cloud data regions only.

You may partially inherit select OCI controls, which can help simplify achieving CMMC Level 3 when running applications on the Oracle US Government Cloud. It is important to understand that using a FedRAMP-accredited cloud does not satisfy every control required by CMMC for a customer tenancy. This guide helps you understand which CMMC controls are your responsibility as well as those that are shared with your managed service provider (MSP) and/or cloud service provider (CSP).

Achieving CMMC Level 3 compliance includes applying controls within your IT environment, personnel, data, and the services you build in your cloud tenancy. Oracle may help you achieve these controls with our cloud native services, features, and enterprise applications or offerings such as PeopleSoft and EBS (HR and/or supply chain) services that you can deploy in Oracle US Government Cloud virtual machines or bare metal. Please refer to product-specific guidance on the vast spectrum of options available from Oracle when you review your solution as it applies to CMMC. CMMC requirements extend to the products you install in your tenancy, how you configure your applications, and how you administer access. For example, if you choose to install a third-party, non-Oracle web server as part of your complete solution, Oracle will not be able to supply guidance on the administration or configuration of that product. Oracle may offer an alternative solution that can be used as part of a CMMC Level 3 certification, and this guide can help you get started.

Tools to Help Achieve CMMC 2.0 Level 3

OCI offers three tools for helping you achieve your CMMC 2.0 Level 3 certification: our OCI Core Landing Zone (LZ), this CMMC Level 3 Guide, and our CMMC Level 3 Controls Checklist. These can be used in combination with the tools you may have used to complete CMMC Level 2.

The Core LZ was designed to leverage native OCI services to create a foundation for customers to deploy a tenancy with an architecture intended to meet stringent government compliance standards. Our Core LZ includes many OCI services for use in your CMMC certification process, and it does not require the installation of additional third-party applications. Our Core LZ wizard creates a tenancy with a foundation of preconfigured native OCI services designed to meet U.S. government compliance standards defined by the NIST 800-172 baseline. Since CMMC level 3 standards are based on NIST 800-172 controls, our Core LZ may help you meet the CMMC 2.0 requirements. While Oracle US Government Cloud has achieved FedRAMP High P-ATO which maps to the NIST 800-172 controls, there are controls shared between you and OCI, and some that are completely your responsibility. This guide describes which controls align with our Core LZ capabilities and how they may help you to meet each control.

Additionally, refer to our CMMC Controls Checklist, which is an editable spreadsheet showing how you may meet CMMC Level 3 compliance controls. Our checklist evaluates each control, shows OCI tools to meet your control obligations, tracks your progress, and helps you address all 24 controls. You may use this checklist in combination with the documentation described in this guide to complete your CMMC documentation for the DIBCAC when required. You should expect a DIBCAC audit to be required if you participate in acquisitions that involve information critical to national security and your tenancy-stored CUI and is designated as requiring CMMC Level 3.

Understanding the CMMC Level 3 Controls

This document has organized the 24 CMMC controls into the following 10 practices. A practice is a categorization or focus area of IT security. The 10 practices are:

1) Access Control (AC): 2 controls
2) Awareness and Training (AT): 2 controls
3) Configuration Management (CM): 3 controls
4) Identification and Authentication (IA): 2 controls
5) Incident Response (IR): 2 controls
6) Personnel Security (PS): 1 control
7) Risk Assessment (RA): 7 controls
8) Security Assessment (CA): 1 control
9) Systems and Communication (SC): 1 control
10) System Information Integrity (SI): 3 controls

Shared Responsibilities

In this section we detail the controls that have a shared responsibility between Oracle and the customer. In addition, this table describes when the Core LZ can help customers meet their obligations for each of the CMMC controls.

CMMC Control	NIST SP 800-172 Control	OCI technology that assists meeting the control	Core LZ deploys OCI tools that can assist meeting the control
Access Control: Organizationally Controlled Assets AC.L3-3.1.2e	3.1.2e	IAM and Containers	N/A
Access Control: Secured Information Transfer AC.L3-3.1.3e	3.1.3e	IAM, Integration Cloud	N/A
Configuration Management: Authoritative Repository CM.L3-3.4.1e	3.4.1e	ORM, Projects, Tags, IAM, VCN, Event Rules, Access Governance	Tags, IAM, VCN, Event Rules, Access Governance
Configuration Management: Automated Detection & Remediation CM.L3-3.4.2e	3.4.2e	IAM, ORM, Cloud Guard, Tags, VCN, and Event rules	Tags, VCN, Event Rules
Configuration Management: Automated Inventory CM.L3-3.4.3e	3.4.3e	IAM, Cloud Guard, Logging	N/A
Identification and Authentication: Bidirectional Authentication IA.L3-3.5.1e	3.5.1e	IAM, Identity, Integration Cloud	N/A
Identification and Authentication: Block Untrusted Assets IA.L3-3.5.3e	3.5.3e	IAM, Identity, Integration Cloud	Cloud Guard, Scripts
Incident Response: Security Operations Center IR.L3-3.6.1e	3.6.1e	NA	N/A
Personnel Security: Adverse Information PS.L3-3.9.2e	3.9.2e	IAM, Identity, Integration Cloud, Events, Cloud Guard	N/A
Risk Assessment: Threat-Informed Risk Assessment RA.L3-3.11.1e	3.11.1e	Cloud Guard, VSS, Monitoring, Events, Audit	N/A
Risk Assessment: Threat Hunting RA.L3-3.11.2e	3.11.2e	Cloud Guard, VSS, Audit	N/A

CMMC Control	NIST SP 800-172 Control	OCI technology that assists meeting the control	Core LZ deploys OCI tools that can assist meeting the control
Risk Assessment: Advanced Risk Identification RA.L3-3.11.3e	3.11.3e	IAM, Cloud Guard, VSS	N/A
Risk Assessment: Security Solution Rationale RA.L3-3.11.4e	3.11.4e	N/A	Tags, Security Lists, VCN, Bastion, Network Security Groups, IAM, Access Governance, 3rd Party Firewalls
Risk Assessment: Security Solution Effectiveness RA.L3-3.11.5e	3.11.5e	Cloud Guard, VSS	N/A
Risk Assessment: Supply Chain Risk Response RA.L3-3.11.6e	3.11.6e	N/A	N/A
Systems and Communications Protection: Isolation SC.L3-3.13.4e	3.13.4e	VCN, SL, NSG, Containers	Security Lists, VCN, Bastion, Network Security Groups, VCN, 3rd Party Firewalls
System and Information Integrity: Integrity Verification SI.L3-3.14.1e	3.14.1e	N/A	N/A
System and Information Integrity: Specialized Asset Security SI.L3-3.14.3e	3.14.3e	WAF, VCN, Containers, Cloud Guard	VCN, 3rd Party Firewalls

CMMC 2.0 Level 3 Guidance for Shared Responsibilities

Our CMMC shared responsibility guidance provides a recommendation for securing your OCI tenancy from an administrator access perspective, the services you build on top of the tenancy, and the solution you provide to end users. Our guide shows when services included in our Core LZ may assist in the achievement of certain controls. When possible, we offer suggestions for Oracle services that may be helpful in meeting a CMMC control. This guide does not provide instructions on the use or configuration of third-party software or tools that you may use inside your tenancy such as Microsoft Active Directory, Okta, virus scanners, and firewalls.

Access Control: Organizationally Controlled Assets AC.L3-3.1.2e

The intent of this control is to ensure that the organization retains ownership, management, and control over system and system components, preventing third parties or individuals from controlling access to sensitive data. OCI can assist with this control by limiting access to sensitive data, not permitting downloads of data, and limiting connections to external systems. Data and users can be segregated with compartments to further limit what is in scope for the control. For additional security, customers can isolate critical workloads by creating child tenancies under a single parent, which provides billing flexibility and improved security posture. Customers can also leverage maximum security zones to maintain a tighter approach by creating and deleting resources within the tenancy. OCI meets this control through Identity and Access Management (IAM) and limiting access to data.

Access Control: Secured Information Transfer AC.L3-3.1.3e

This control is intended to facilitate secure information transfer between security domains, ensuring that specific CMMC Level 3 data is not transferred to components or systems that do not employ the required security. OCI offers capabilities such as compartments, tags, and vast database (DB) tools to ensure data transfer is controlled—IAM can help you control user access to the data or the systems that manage the data. OCI also supports this control via native TLS 1.2 encryption, enabling customers to enhance traffic control, especially north-south traffic, using Network Security Groups (NSG) and security lists. For data transfer, customers can use IPSec over FastConnect for encrypting data to send in and out of the cloud. Oracle US Government Cloud is not connected to systems that have not achieved FedRAMP accreditation, which includes this control.

Configuration Management: Authoritative Repository CM.L3-3.4.1e

This control requires the establishment and maintenance of an authoritative repository and source to provide accountability for approved system components. OCI offers multiple tools to assist in meeting this control, including OCI Resource Manager (ORM), Projects, Tags, IAM, Event Rules, and Access Governance. OCI services like Object Storage, Resource Manager can be used to securely store and version-control system configurations, baselines, and infrastructure-as-code templates. OCI operations and support staff meet this control for our internal control plane and code management.

The Core LZ can perform the following:

- Deploy the following two default tags:
    - Created By tag, which identifies who created the resource
    - Created On tag, which identifies when the resource was created
- Support customer-provided tags
- Support the CIS Compliance Checker script, which can be run in an OCI tenancy to query all resources and output them as JSON
- Change authentication settings
- Deploy Virtual Cloud Networks (VCN) that can be used for deploying compute Instances, and the Secure Workload Module deploys compute instances with Secure Boot and in-transit encryption enabled
- Create an OCI event rules for network gateway changes
- Create an OCI event rule for network security group changes
- Create an OCI event rule for VCN changes
- Create an OCI event rule for IDP mapping changes
- Create an OCI event rule for network route table changes
- Create an OCI event rule for IAM policy changes
- Create an OCI event rule for IAM User changes
- Create an OCI event rule for network security list changes
- Create an OCI event rule for IAM group changes
- Create an OCI event rule for Identity Provider changes
- By default, Oracle Cloud Infrastructure supports federation with Oracle Identity Cloud Service, and Microsoft Active Directory (via Active Directory Federation Services (AD FS)), Microsoft

Azure Active Directory, Okta, and other identity providers that supports the Security Assertion Markup Language (SAML) 2.0 protocol

- Optionally deploy the OCI IAM policies for deploying an Oracle Access Governance instance to govern OCI IAM and other Identity systems

Configuration Management: Automated Detection & Remediation CM.L3-3.4.2e

This control seeks to enforce the use of automation to detect misconfigured or unauthorized system components. After detection, these components should be removed or quarantined for remediation, patching, re-configuration, or other mitigation. OCI tools that can help you meet this control include IAM, ORM, Cloud Guard, Tags, VCN, and Event Rules. OCI operations and support staff meet this control for our internal control plane and system management tools.

The Core LZ can perform the following:

- Change authentication settings
- Deploy VCNs that can be used for deploying compute Instances, and the Secure Workload Module deploys compute instances with Secure Boot and in-transit encryption enabled.
- Create an OCI event rules for network gateway changes
- Create an OCI event rule for network security group changes
- Create an OCI event rule for VCN changes
- Create an OCI event rule for IDP mapping changes
- Create an OCI event rule for network route table changes
- Create an OCI event rule for IAM policy changes
- Create an OCI event rule for IAM user changes
- Create an OCI event rule for network security list changes
- Create an OCI event rule for IAM group changes
- Create an OCI event rule for Identity Provider changes

Configuration Management: Automated Inventory CM.L3-3.4.3e

This control requires the use of automated management and discovery tools to create and maintain a current, complete, accurate and accessible inventory of system components. OCI tools that can help include IAM, Cloud Guard, and Logging. OCI maintains such an inventory for our cloud operations and support.

Identification and Authentication: Bidirectional Authentication IA.L3-3.5.1e

Prior to connecting to the network, this control requires the bidirectional identification and authentication of system and system components using cryptography that is replay resistant. OCI offers tools that can assist in meeting this control such as IAM, Multifactor Authentication (MFA), Network Security Groups, security lists), Identity, and Integration Cloud. Leveraging OCI's Audit service alongside Functions allows customers to automatically monitor, authorize, and trigger alerts for access events, providing real-time visibility and control over who is granted access. OCI ensures such cryptography, authentication, and identification techniques are used for our cloud operations and support.

Identification and Authentication: Block Untrusted Assets IA.L3-3.5.3e

This control requires the use of automated or manual and procedural methods to prevent components from connecting to the organizational system unless they are known and authenticated with the appropriate configuration state and trusted profile. OCI offers tools that can assist in meeting this control such as IAM, Identity, and Oracle Integration Cloud. OCI uses such methods to validate components for our cloud operations and support prior to allowing connection.

The Core LZ can perform the following:

- When Cloud Guard is enabled, a target is provided for the root compartment with the out-of-box configuration, activity detector recipes, and responder recipes
- Support the CIS Compliance Checker script, which can be run in an OCI tenancy to query all resources and output them as JSON

Incident Response: Security Operations Center IR.L3-3.6.1e

This control requires the creation and on-going operation of a 24/7 security operations center or a remote/on-call staff. OCI does not offer tools that can assist in meeting this control; however, customers can leverage OCI's services such as Audit, Cloud Guard, Logging, and other security services to support real-time threat detection and incident notification. OCI provides tools that can provide third party SIEM integration for a centralized incident detection and response solution. OCI maintains a 24/7 security operations center.

Personnel Security: Adverse Information PS.L3-3.9.2e

This control requires that the organizational systems are protected in the event that adverse information is discovered about individuals with access to CUI. There are several OCI tools that can assist with meeting this control, including IAM, Identity, Oracle Integration Cloud, Events, and Cloud Guard. OCI operations and support staff monitor users and adhere to this control, but they have no visibility or access to customer CUI.

Risk Assessment: Threat-Informed Risk Assessment RA.L3-3.11.1e

This control requires organizations to incorporate current cyber threat intelligence (CTI) into their risk assessment processes. The intent is to ensure that the assessment of risks to systems, data, and operations reflects real-world adversary tactics, techniques, and procedures (TTPs), rather than relying solely on static or historical data. In an OCI tenancy, this is achieved using multiple services mainly by integrating threat intelligence into Cloud Guard and security zones. Cloud Guard detector recipes are regularly updated based on evolving threat patterns and known attack vectors allowing organizations to assess their security posture not just against best practices but with respect to the emerging threats. OCI operations uses multiple tools to track evolving threats and respond accordingly.

Risk Assessment: Threat Hunting RA.L3-3.11.2e

This control requires organizations to proactively search for indicators of compromise (IOCs) or adversary behavior that may evade automated detection. Unlike reactive monitoring, threat hunting relies on hypothesis-driven investigation and correlation of subtle signals across systems. OCI offers services to help satisfy the control such as Logging Analytics and Cloud Guard. Logging Analytics aggregates logs from compute, network, identity, and database layers, allowing analysts to build complex queries and detect anomalous patterns over time. Cloud Guard continuously analyzes resources configuration, network activity, and user behavior to surface suspicious activity. OCI operations uses multiple threat hunting tools and responds accordingly.

Risk Assessment: Advanced Risk Identification RA.L3-3.11.3e

The control emphasizes the need for organizations to proactively identify advanced persistent threats (APTs), zero-day vulnerabilities, and emerging risks that may not be captured by traditional risk assessments. The control requires ongoing analysis of current threat intelligence and system behavior to detect complex and evolving attack patterns. OCI helps customers addresses this requirement through a combination of telemetry such as threat intel and automated detection capabilities. Oracle Logging

Analytics and security monitoring extend this capability by enabling pattern-based anomaly detection across application, infrastructure, and network logs. Also, Cloud Guard not only evaluates configurations and activities against known baselines but also integrates with threat intelligence service. OCI operations uses multiple tools to track advanced persistent threats and responds accordingly.

Risk Assessment: Security Solution Rationale RA.L3-3.11.4e

This control requires organizations to document and justify the selection of security solutions, ensuring they are appropriate for addressing identified risks and aligned with organizational security objectives. The rationale must be based on expected effectiveness, threat data, and system criticality.

OCI customers can implement Cloud Guard, Data Safe, Vulnerability Scanning, and Security Zones to help meet this control. Risk-based design services like Cloud Guard and Data Safe are purpose-built to address specific threat vectors (e.g., misconfigurations, data exposure), and Oracle publishes best practices explaining when and why to use them. Oracle recommends a layered defense approach and allows organizations to define policies and compartmentalization based on the sensitivity of workloads ensuring selected tools align with threat likelihood and impact. This approach satisfies the control by ensuring all security controls have traceable, risk-informed justifications aligned to operational context and compliance objectives. OCI operations staff document and align policies to ensure security alignment.

The Core LZ can perform the following:

- Deploy the following two default tags:
    - Created By tag, which identifies who created the resource
    - Created On tag, which identifies when the resource was created
- Support customer-provided tags
- Support the CIS Compliance Checker script, which can be run in an OCI Tenancy to query all resources and output them as JSON
- Create a security list for each VCN it creates
    - The security only allows port 22 connections from on-premises CIDRs or the hub network
    - The on-premises CIDRs variable does not allow 0.0.0.0/0
- Deploy a bastion NSG for each VCN it creates
    - That NSG allows ports 22 and 3389; however, the variable for ingress CIDRs does not allow 0.0.0.0/0.
- Create a security list for each VCN it creates.
    - The security only allows port 22 connections from on-premises CIDRs or the hub network.
    - The on-premises CIDRs variable does not allow 0.0.0.0/0.
- Optionally deploy the OCI IAM policies for deploying an Oracle Access Governance instance to govern OCI IAM and other Identity Systems
- By default, OCI supports federation with Oracle Identity Cloud Service, and Microsoft Active Directory (via AD FS), Microsoft Azure Active Directory, Okta, and other identity providers that supports the SAML 2.0 protocol
- Deploy three subnets: one to host load balancers and bastion hosts, one for application servers (middle-tiers) and one for database servers
    - The load balancer subnet can be made either public or private
    - The application servers and database servers are always created private

    - Route rules and network security rules are configured based on provided connectivity settings
- Deploy network security devices like third party Next Generation Firewalls from Checkpoint, Cisco, Fortinet, and Palo Alto Networks or the OCI Network Firewall, all of which are available in the OCI Marketplace.
    - The architecture funnels all traffic to these network security devices to leverage their security capabilities centrally
- Deploy VCNs with database subnets, which are private that can be used for deploying an ADB-S or OAC instances.
- By default, the Network Visualizer provides a diagram of the implemented topology of all VCNs in a selected region and tenancy.

Risk Assessment: Security Solution Effectiveness RA.L3-3.11.5e

This control requires assessing the effectiveness of security solutions at least annually or upon relevant threat intelligence or incident to ensure they address anticipated risks based on current and accumulated threat data. OCI customers can meet these using services such as Cloud Guard, which continuously evaluates configurations and detector rule effectiveness, surfacing gaps and remediations. Data Safe Security Assessments automatically run weekly, reporting configuration drift, user risk, and control efficacy for databases. Using security zones and Logging Analytics enforce guardrails and provide audit-ready reports for annual validation. OCI operations staff regularly assess the effectiveness of our security solutions.

Risk Assessment: Supply Chain Risk Response RA.L3-3.11.6e

This control mandates that organizations assess, respond to, and monitor supply chain risks affecting systems and components. Oracle publishes a comprehensive Supply Chain Risk Management (SCRM) plan as part of Oracle's SCRM program that can assist in meeting this control. OCI operations staff regularly assess cloud supply chain risks.

Systems and Communications Protection: Isolation SC.L3-3.13.4e

This control mandates that CUI and supporting services be segregated physically and/or logically to limit unauthorized data flows, reduce attack surface, and impede adversary movement across system components. OCI offers isolation to segregate CUI and reduce attack surfaces through a combination of network, compute, and compartmentalization. VCNs and subnets create isolated network domains for CUI workloads, with private subnets, route tables, NSGs, and compartments to enforce boundary protection. For even more data isolation, child tenancies can be created so the workloads can be kept dedicated and not shared with other mission owners. Dedicated and private endpoints leverage private service connections and service gateways to access OCI services (e.g., Object Storage) without traversing the public internet. OCI operations and support staff do not have access to CUI workloads hosted in Your Content.

The Core LZ can perform the following:

- Create a security list for each VCN it creates
    - The security only allows port 22 connections from on-premises CIDRs or the hub network
    - The on-premises CIDRs variable does not allow 0.0.0.0/0
- Deploy a bastion NSG for each VCN it creates
    - That NSG allows ports 22 and 3389; however, the variable for ingress CIDRs does not allow 0.0.0.0/0

- Deploy VCNs with database subnets, which are private subnets that can be used for deploying ADB-S or OAC instances
- Create a security list for each VCN it creates
    - The security only allows port 22 connections from on-premises CIDRs or the hub network
    - The on-premises CIDRs variable does not allow 0.0.0.0/0
- Deploy three subnets, one to host load balancers and bastion hosts, one for application servers (middle-tiers) and one for database servers
    - The load balancer subnet can be made either public or private
    - The application servers and database servers are always created private
    - Route rules and network security rules are configured based on provided connectivity settings
- Deploy network security devices like third party Next Generation Firewalls from Checkpoint, Cisco, Fortinet, and Palo Alto Networks or the OCI Network Firewall
    - The architecture funnels all traffic to these network security devices to leverage their security capabilities centrally

System and Information Integrity: Integrity Verification SI.L3-3.14.1e

This control requires integrity verification of system components and information. OCI's security architecture includes cryptographic integrity checks, automated patch management, and continuous monitoring to detect unauthorized changes or corruption. OCI provides built-in tools to assist in meeting this control such as Oracle Cloud Guard, Logging, and auditing to track system and data integrity events in real-time.

OCI's immutable infrastructure and automated image verification during deployment ensure that only validated, trusted system components are used. Integration with Key Management Service (KMS) supports cryptographic verification such as digital signatures and hash verification, to authenticate and verify data integrity for stored and in-transit data. Compute instances leverage secure boot process and TPMs (Trusted Platform Module) to validate the integrity of boot firmware and operating systems ensuring only trusted code is executed during start up.

System and Information Integrity: Specialized Asset Security SI.L3-3.14.3e

This control requires specialized assets (including IT, IoT, OT, GFE, restricted and test equipment) to be included in scope for enhanced security or are segregated in specified networks. OCI can assist in meeting this control by applying purpose-built protections for high-value resources. OCI Vault provides Hardware Security Modules (HSMs) certified to FIPS 140-2 Level 3 for cryptographic key generation, storage, and usage, ensuring keys never leave secure boundaries. Dedicated Bare Metal and Virtual Machine instances can be deployed within private subnets and isolated compartments, with customizable security policies to restrict administrative access. OCI's Security Zones enforce guardrails that automatically validate compartment and resource configurations against organizational standards, preventing deployment of unsupported or misconfigured specialized assets. Continuous configuration monitoring via Cloud Guard and Logging Analytics ensures any deviation triggers alerts and automated remediation. This multi-layered, asset-specific approach guarantees that critical workloads and cryptographic materials maintain integrity, confidentiality, and availability throughout their lifecycle. OCI operations and support ensure all OCI assets, including specialized assets meet any required enhanced security.

The Core LZ can perform the following:

- By default, Oracle Cloud Infrastructure supports federation with Oracle Identity Cloud Service, and Microsoft Active Directory (via AD FS), Microsoft Azure Active Directory, Okta, and other identity providers that supports the SAML 2.0 protocol
- Deploys three subnets, one to host load balancers and bastion hosts, one for application servers (middle-tiers) and one for database servers
  - The load balancer subnet can be made either public or private
  - The application servers and database servers are always created private
  - Route rules and network security rules are configured based on provided connectivity settings
- Deploy network security devices like third party Next Generation Firewalls from Checkpoint, Cisco, Fortinet, and Palo Alto Networks or the OCI Network Firewall
  - The architecture funnels all traffic to these network security devices to leverage their security capabilities centrally

Customer Owned Responsibilities

In this section we detail the controls that are owned the customer.

CMMC Control	NIST SP 800-172 Control	OCI technology that assists meeting the control	Core LZ deploys OCI tools that can assist meeting the control
Awareness and Training: Advanced Threat Awareness AT.L3-3.2.1e	3.2.1.e	N/A	N/A
Awareness and Training: Practical Training Exercises AT.L3-3.2.2e	3.2.2e	N/A	N/A
Incident Response: Cyber Incident Response Team IR.L3-3.6.2e	3.6.2.e	NA	N/A
Risk Assessment: Supply Chain Risk Plan RA.L3-3.11.7e	3.11.7e	N/A	N/A
Security Assessment: Penetration Testing CA.L3-3.12.1e	3.12.1e	N/A	N/A
System and Information Integrity: Threat-Guided Intrusion Detection SI.L3-3.14.6e	3.14.6e	N/A	N/A

CMMC 2.0 Level 3 Guidance for Customer Responsibilities

Our CMMC customer responsibility guidance provides a description of each control and a high-level recommendation for securing your OCI tenancy and certifying the services you build on top of the tenancy in the delivery of the solution you provide to your end users. Our guide shows when services included in our Core LZ may assist in the achievement of certain controls. When possible, we offer suggestions for Oracle services that may be helpful in meeting a CMMC control. This guide does not provide instructions on the use or configuration of third-party software or tools that you may use inside your tenancy such as Microsoft Active Directory, Okta, virus scanners, and firewalls, nor process control such as employee training.

Awareness and Training: Advanced Threat Awareness AT.L3-3.2.1e

This control drives awareness of threats through training sessions to educate employees on social engineering, advanced persistent threat actors, breaches, and suspicious behaviors. Advanced threat awareness training is provided during the new employee onboarding process, after a significant cyber event, or at least once per year. OCI does not provide tools to facilitate training, but customers can use OCI Identity tools to track which individuals may have access to CUI or CMMC Level 3 specified data. OCI operations and support staff receive this level of training.

Awareness and Training: Practical Training Exercises AT.L3-3.2.2e

This control is intended to ensure practical exercises are included in awareness training for all users, are customized to user roles as they relate to current threat scenarios, and include feedback to the participants and their supervisors. OCI does not offer tools to facilitate training, but OCI Identity tools can be used to track which individuals may have access to CUI or CMMC Level 3 specified data. OCI operations and support staff receive this level of training.

Incident Response: Cyber Incident Response Team IR.L3-3.6.2e

This control requires the creation and on-going operation of a cyber incident response team that can be deployed by the organization within 24 hours of an incident. OCI does not offer tools that can assist in meeting this control. OCI maintains a cyber incident response team available within 24 hours of an incident for purposes of FedRAMP compliance.

Risk Assessment: Supply Chain Risk Plan RA.L3-3.11.7e

This control requires organizations to develop and maintain a documented plan for identifying, assessing, and mitigating risks in their supply chains, updating it annually and whenever relevant cyber threat or incident information arises. Oracle publishes a comprehensive SCRM plan as part of Oracle's SCRM program that can assist in meeting this control.

Security Assessment: Penetration Testing CA.L3-3.12.1e

This control mandates penetration testing annually or when there is significant change using both automated scanning tools and subject matter expert (SME) ad hoc tests to uncover exploitable vulnerabilities. OCI offers the Vulnerability Scanning service for routine host and container image assessments, that seamlessly integrates with Cloud Guard for centralized detection, alerting, and remediation workflows. Oracle's Customer Security Testing Policy then provides the framework and pre-approval process under which customers may perform penetration tests against their cloud tenancy and access detailed test summaries under NDA (non-disclosure agreement), ensuring thorough security validation with minimal operational impact. OCI operations conducts internal penetration testing as needed or annually.

System and Information Integrity: Threat-Guided Intrusion Detection SI.L3-3.14.6e

This control requires organizations to implement intrusion detection capabilities that are informed by current cyber threat intelligence. The intent is to ensure that Intrusion Detection Systems (IDS) are not generic or static but dynamically updated to detect adversary behaviors based on evolving threat data and attack techniques. Customers can leverage OCI's threat-guided intrusion detection framework in order to maintain system and information integrity under control. Security services such as OCI Cloud Guard continuously feed telemetry—network flow logs, audit trails, host metrics and applies threat intelligence and machine-learning models to identify anomalous activity in real time and responding to alerts and taking action. The integrated IDS monitors east-west and north-south traffic, detecting known signatures and behavioral abnormalities without impacting performance. Host-level agents (OS Management and Logging Analytics) supplement network detection by flagging unusual processes, file changes, or privilege escalations. When indicators of compromise arise such as unexpected lateral movement or exploitation attempts OCI automatically generates alerts, applies risk scoring, and can trigger responsive actions (network isolation, WAF rule deployment, or automated remediation). This layered, threat-centric approach ensures that intrusion detection is guided by evolving adversary tactics, minimizing dwell time, and preserving the confidentiality, integrity, and availability of cloud workloads. Oracle leverages intrusion detection based on current threats for the operation and support of the OCI cloud.

Using the OCI Core Landing Zone

This OCI Core LZ Architecture Guide provides an overview of how organizations can use OCI to comply with the CMMC requirements. This guide is intended to help administrators understand OCI's capabilities and plan IT projects that leverage OCI Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offerings to build a CMMC-compliant ecosystem. This guide refers to the OCI Core LZ, which has been validated by the Center for Internet Security (CIS) to assist customers in meeting their portion of the CMMC control in the shared responsibility matrix.

OCI Core LZs are pre-configured, secure, scalable environments that serve as a starting point for deploying workloads in the cloud using standard Terraform. The OCI Core LZ is specifically designed to help organizations meet CMMC requirements efficiently. To access the Core LZ assets, administrators should navigate to the OCI LZs GitHub repository found here: https://github.com/oci-landing-zones/terraform-oci-core-landingzone.

The GitHub repository will provide the customer with the Terraform scripts to create the Core LZ. This repository also includes a README document with detailed instructions, architectural layouts, technical diagrams, release notes, and other supporting documents.

By leveraging the OCI Core LZ, organizations can rapidly deploy a secure, compliant environment, saving time and reducing the complexity of meeting CMMC requirements in the cloud.

How to Complete CMMC Level 3 Certification

Please refer to this CMMC site for next steps on completing CMMC certification: https://dodcio.defense.gov/CMMC/Assessments/.

Resources

- Oracle Government Cloud documentation
- Oracle Cloud for Government
- Oracle Government Cloud for Contractors
- Base Database Security
- Identity and Access Management on Exadata Database on Dedicated Infrastructure
- Oracle Database User Identity and Access Management with Base Database Service
- Core Landing Zone
- CMMC Level 1 Guide
- CMMC Level 1 Checklist
- CMMC Level 2 Guide
- CMMC Level 2 Checklist
- Oracle Cloud Infrastructure Identity Domains
- CMMC website
- CMMC Self-Assessment Guide on the CMMC website
- CMMC Accreditation Body

Terms and Acronyms

3PAO	Third Party Assessment Organization
AC	Access Control
AD FS	Active Directory Federation Services
ADB	Autonomous Database
ADB-S	Autonomous Shared Database
APT	Advanced Persistent Threats
AT	Awareness and Training
AU	Audit and Accountability
BM	Bare Metal
CA	Security Assessment
CIDR	Classless Inter-Domain Routing
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CM	Configuration Management
CMK	Customer Managed Key
CMMC	Cybersecurity Maturity Model Certification
CSP	Cloud Service Provider
CTI	Cyber Threat Intelligence
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposure
CVSS	Common Vulnerabilities Scoring System
CWE	Common Weakness Enumeration
DB	Database
DbaaS	Database as a Service (BaseDB)
DIB	Defense Industrial Base
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center
DMZ	Demilitarized Zone
DoD	Department of Defense
DRG	Dynamic Routing Gateway
FCI	Federal Contract Information
FedRAMP	Federal Risk and Authorization Program
FSS	File Storage Service
HSM	Hardware Security Module
IA	Identification and Authentication

IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IDS	Intrusion Detection Systems
IOC	Indicators of Compromise
IR	Incident Response
ISAC	Information Sharing and Analysis Center
IT	Information Technology
KMS	Key Management Service
LZ	Landing Zone
MA	Maintenance
MFA	Multifactor Authentication
MP	Media Protection
MSP	Managed Service Provider
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NSG	Network Security Group
NVD	National Vulnerability Database
OAC	Oracle Analytics Cloud
OCI	Oracle Cloud Infrastructure
ORM	OCI Resource Manager
OS	Operating System
OVAL	Open Vulnerability Assessment Language
PaaS	Platform as a Service
PE	Physical Protection
PS	Personnel Security
RA	Risk Assessment
RBAC	Role Based Access Control
SAML	Security Assertion Markup Language
SC	Systems and Communications
SCAP	Security Content Automated Protocol
SCH	Service Connector Hub
SCRM	Supply Chain Risk Management
SI	System Information Integrity
SME	Subject Matter Expert
SSP	System Security Plan

TPM	Trusted Platform Module
TTP	Tactics, Techniques, and Procedures
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
UTC	Coordinated Universal Time
VCN	Virtual Cloud Network
VDMS	Virtual Data Center Managed Services
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VSS	Vulnerability Scanning Service
WAF	Web Application Firewall

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   x.com/oracle