ORACLE

Oracle U.S. Government Cloud & CMMC 2.0 Level 2 Informational Guide

Informational Guide to Assist Customer with CMMC 2.0 Level 2 compliance

October, 2024, Version [1.0]

Public

Purpose statement

This document is designed to provide basic guidance to the Defense Industrial Base community needing to achieve Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 2 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.

ORACLE

Table of contents

ORACLE

Introduction

This basic guide is designed to assist the Defense Industrial Base (DIBs) that will pursue CMMC Level 2 certification. DIBs that store Federal Contract Information (FCI), and not Controlled Unclassified Information (CUI), must meet CMMC 2.0 Level 1 requirements. However, DIBs that store CUI will be held to the CMMC Level 2 standard and will need to assess against additional CMMC controls and likely will require a Third Party Assessment Organization (3PAO) to independently assess the environment's security posture. You need to review the data you store and manage as part of your government contracts to determine the level of CMMC compliance that applies to you. Compliance with CMMC 2.0 Level 1 includes 15 controls, which align with 17 FedRAMP and NIST 800-171 controls. CMMC Level 2 expands to 110 controls. Oracle US Government Cloud has achieved FedRAMP High JAB P-ATO, which means that Oracle Cloud Infrastructure (OCI) services running within Oracle US Government Cloud data regions meet NIST 800-171 control requirements. All OCI references are to the Oracle U.S. Government Cloud data region only.

You may inherit select OCI controls and simplify the achievement of CMMC Level 2 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 2 compliance includes applying controls within your cloud environment, personnel, data, and the services you build in your cloud tenancy. Oracle may help you achieve these controls with our cloud native services and features as well as other enterprise applications or offerings such as PeopleSoft and EBS (HR and/or supply chain) services you can deploy in 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 2 certification, and this guide can help you get started.

ORACLE

Tools to Help Achieve CMMC 2.0 Level 2

OCI offers three tools for helping you achieve your CMMC 2.0 Level 2 certification: our OCI Core Landing Zone (LZ), this CMMC Level 2 Guide, and our CMMC Level 2 Controls Checklist.

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 SP800-171 baseline. Since CMMC standards are based on NIST 800-171 controls, our Core LZ may help you meet the CMMC 2.0 requirements. While Oracle US Government Cloud has achieved FedRAMP High JAB P-ATO, 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.

Our attached CMMC Controls Checklist is an editable spreadsheet showing how you may meet CMMC Level 2 compliance controls. Our checklist evaluates each control, shows OCI tools to meet your control obligations, tracks your progress, and helps you address all 110 controls. You may use this checklist in combination with the documentation described in this guide to complete your CMMC documentation for your Third Party Assessment Organization (3PAO) when required. You should expect a 3PAO audit to be required if you participate in acquisitions that involve information critical to national security and your tenancy-stored CUI.

ORACLE

Understanding the CMMC Level 2 Controls

This document has organized the 110 CMMC controls into the following three categories:

1) Controls that are typically the responsibility of the CSP
2) Controls that are the shared responsibility of the CSP and the customer
3) Controls that are the responsibility of the customer

Within the three categories mentioned above, the controls are divided into 14 practices. A practice is a categorization or focus area of IT security. The 14 practices are:

1) Access Control (AC): 22 controls
2) Awareness and Training (AT): 3 controls
3) Audit and Accountability (AU): 9 controls
4) Configuration Management (CM): 9 controls
5) Identification and Authentication (IA):11 controls
6) Incident Response (IR): 3 controls
7) Maintenance (MA): 6 controls
8) Media Protection (MP): 9 controls
9) Personnel Security (PS): 2 controls
10) Physical Protection (PE): 6 controls
11) Risk Assessment (RA): 3 controls
12) Security Assessment (CA): 4 controls
13) Systems and Communication (SC): 16 controls
14) System Information Integrity (SI): 7 controls

ORACLE

OCI Responsibilities

While OCI can provide the controls listed below, if you have a hybrid or on-premises cloud solution, you may need to evaluate your posture against these controls. For example, if you own media disposal controls for data downloaded to local devices (e.g., laptops or USB drives), preventing users from downloading data may be necessary.

CMMC Domain and Control	NIST SP 800-171 Control	Summary
Maintenance: Perform Maintenance MA.L2-3.7.1	3.7.1	Implement maintenance on Organizational Systems
Maintenance: System Maintenance Control MA.L2-3.7.2	3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
Maintenance: Equipment Sanitation MA.L2-3.7.3	3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.
Maintenance: Media Inspection MA.L2-3.7.4	3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
Maintenance: Maintenance Personnel MA.L2-3.7.6	3.7.6	Supervise the maintenance activities of personnel without required access authorization.
Media Protection: Media Protection MP.L2-3.8.1	3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
Media Protection: Media Access MP.L2-3.8.2	3.8.2	Limit access to CUI on system media to authorized users.
Media Protection: Media Disposal MP.L2-3.8.3	3.8.3	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
Media Protection: Media Markings MP.L2-3.8.4	3.8.4	Mark media with necessary CUI markings and distribution limitations.
Media Protection: Media Accountability MP.L2-3.8.5	3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
Media Protection: Portable Storage Encryption MP.L2-3.8.6	3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
Media Protection: Removeable Media MP.L2-3.8.7	3.8.7	Control the use of removable media on system components.
Media Protection: Shared Media MP.L3-3.8.8	3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.

CMMC Domain and Control	NIST SP 800-171 Control	Summary
Media Protection: Protect Backups MP.L2-3.8.9	3.8.9	Protect the confidentiality of backup CUI at storage locations.
Physical Protection: Limit Physical Access PE.L2-3.10.1	3.10.1	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
Physical Protection: Monitor Facility PE.L2-3.10.2	3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.
Physical Protection: Escort Visitors PE.L2-3.10.3	3.10.3	Escort visitors and monitor visitor activity.
Physical Protection: Physical Access Logs PE.L2-3.10.4	3.10.4	Maintain audit logs of physical access.
Physical Protection: Manage Physical Access PE.L2-3.10.5	3.10.5	Control and manage physical access devices.

CMMC Level 2 Control Descriptions: OCI Responsibilities

Maintenance: Perform Maintenance MA.L2-3.7.1

This control focuses on implementing automated maintenance capabilities for system updates, patches, and security fixes.

Oracle Cloud Infrastructure (OCI) provides automated maintenance capabilities through its OCI operations team. Maintenance capabilities include regular updates, patches, and security fixes for the underlying infrastructure. Oracle implements automated maintenance windows for services like Oracle Database Cloud Service to ensure system maintenance is performed periodically. OCI operations uses rigid and auditable identity tools to manage the control plane, conduct administration, and deliver customer support, all of which contribute to secure maintenance practices.

Maintenance: System Maintenance Control MA.L2-3.7.2

This control ensures tools, techniques, mechanisms, and personnel used for maintenance procedures are in place. Customers may need to configure their OCI environment to align with their organization's remote maintenance policies. OCI operations uses rigid and auditable tools to perform maintenance on the control plane, conduct administration, and deliver customer support, all of which contribute to secure maintenance practices.

OCI implements secure remote maintenance capabilities through management consoles and APIs. OCI's Identity and Access Management (IAM) is used to control and monitor remote maintenance activities, including enforcing multifactor authentication for remote maintenance sessions. Access for maintenance is provided using a least privilege model, ensuring that maintenance personnel have only the capabilities necessary to complete their designated tasks.

Maintenance: Equipment Sanitization MA.L2-3.7.3

This control requires the sanitization of any equipment removed for off-site maintenance. In the cloud context, this primarily relates to logging and auditing maintenance activities. OCI operations uses approved sanitation tools prior to removing any media from our cloud environment and prior to performing maintenance on equipment used in the control plane, to conduct administration, and to deliver customer support, all of which contribute to secure maintenance practices.

Maintenance: Media Inspection MA.L2-3.7.4

This control focuses on protecting media containing test/diagnostic programs for malicious code prior to use in the environment and, if found, directing it through incident handling processes. Customers may need to review and configure test and diagnostic tools used in their OCI environment. OCI operations inspects and reviews all media used in cloud operations, and also manages supply chain of media to manage the control plane, conduct administration, and delivery of customer support. Access is granted with separation of duty as a priority.

Network security groups and security lists are configured to restrict access to maintenance interfaces. Additionally, OCI Virtual Cloud Networks (VCNs) are used to isolate maintenance traffic. All remote access for managing the control plane, conducting administration, and delivering customer support is restricted, aligning with the principle of limiting access points.

Maintenance: Maintenance Personnel MA.L2-3.7.6

This control requires supervision of maintenance activities and personnel for those without authorized access.

OCI operations provides mechanisms to supervise maintenance activities. Monitoring capabilities are enhanced by the use of rigid and auditable identity tools, ensuring that all maintenance activities are properly tracked and supervised.

Media Protection: Media Protection MP.L2-3.8.1

This control focuses on protecting system media containing CUI. OCI operations has no access to a customer's content that contains CUI, but all customer and cloud operations data is protected using required physical access controls access is limited to properly trained and authorized US citizens.

OCI provides robust mechanisms for protecting system media containing CUI, both paper and digital. The Core LZ deploys an optional OCI Vault in the Security Compartment and generates an optional Customer Managed Key (CMK). The LZ also deploys required OCI IAM policies for Object Storage, Block Volume, and File Storage services, enhancing the protection of stored data.

The Core LZ can help customers manage Object, Block, and File storage. To assist protecting system media containing CUI in both paper and digital forms, the following Core LZ options have been established. Depending on the use case, the Core LZ can assist with some potential customer-owned controls, as described in the following paragraphs.

The Core LZ deploys an optional (Level 2 selected) OCI Vault in the Security Compartment and generates an optional CMK. It also deploys required OCI IAM policies for the Object Storage service and OCI IAM groups to use CMKs in the Security Compartment. The Core LZ deploys an optional Object Storage bucket in the AppDev Compartment. That bucket is deployed with versioning enabled. It also deploys required OCI IAM policies for the Block Volume service and OCI IAM groups to use CMKs in the Security Compartment. It also deploys required OCI IAM policies for the File Storage Service (FSS) and OCI IAM groups to use keys in the Security Compartment.

Media Protection: Media Access MP.L2-3.8.2

This control limits access to CUI on system media to authorized users.

OCI operations has no access to customer content with CUI, but OCI implements strong access controls to limit access to all data on system media to only authorized users.

To assist customers in the logical access to their own CUI, the Core LZ defines various personas with specific access rights, including IAM Administrators, Credential Administrators, and Security Administrators. These roles are implemented using OCI IAM, ensuring least privilege access.

The Core LZ can also assist with IAM and Object storage. To limit access to CUI on system media to authorized users, the following actions have been taken by the Core LZ.

Depending on use case, the Core LZ can assist with some potential customer-owned controls, as described in the following paragraphs.

The Core LZ defines the following personas that account for most organizational needs:

- IAM Administrators: manage IAM services and resources including compartments, groups, dynamic groups, policies, identity providers, authentication policies, network sources, tag defaults. However, this group is not allowed to manage the out-of-box Administrators and Credential Administrators groups or modify the out-of-box Tenancy Admin policy.
- Credential Administrators: manage users capabilities and users credentials in general, including API keys, authentication tokens and secret keys.
- Cost Administrators: manage budgets and usage reports.
- Auditors: entitled with read-only access across the tenancy and the ability to use cloud-shell to run the cis_reports.py script.
- Announcement Readers: for reading announcements displayed in OCI Console.
- Security Administrators: manage security services and resources including Vaults, Keys, Logging, Vulnerability Scanning, Web Application Firewall, Bastion, Service Connector Hub.
- Network Administrators: manage OCI network family, including VCNs, Load Balancers, DRGs, VNICs, IP addresses.
- Application Administrators: manage application related resources including Compute images, OCI Functions, Kubernetes clusters, Streams, Object Storage, Block Storage, File Storage.
- Database Administrators: manage database services, including Oracle VMDB (Virtual Machine), BMDB (Bare Metal), ADB (Autonomous databases), Exadata databases, MySQL, NoSQL, etc.
- ExaCS Administrators (only created when ExaCS compartment is created): manage Exadata infrastructure and VM clusters in the ExaCS compartment.
- Storage Administrators: the only group allowed to delete storage resources, including buckets, volumes, and files. Used as a protection measure against inadvertent deletion of storage resources.

The Core LZ also deploys an optional Object Storage bucket(s) in the AppDev Compartment. Those bucket(s) are deployed as a private bucket.

Media Protection: Media Disposal MP.L2-3.8.3

This control requires sanitization or destruction of system media containing CUI before disposal or release for reuse.

For customers managing CUI in their tenancy, OCI provides secure data deletion capabilities for its storage services. For Object Storage, OCI offers Object Lifecycle Management for automatic deletion or archiving. Block Volumes include volume termination protection and secure volume wiping. File Storage service supports secure deletion of file systems and snapshots. OCI operations uses rigid and auditable tools to manage these processes and ensures all media containing customer data is physically destroyed.

Media Protection: Media Markings MP.L2-3.8.4

This control involves marking media with necessary CUI markings and distribution limitations. Customers are responsible for determining the appropriate markings for their CUI. OCI provides tagging capabilities for logically marking and categorizing digital media containing CUI. These tags can be used in conjunction with IAM policies to control access to CUI-containing resources, adhering to the principle of least privilege. OCI operations has no access to customer content with CUI and uses rigid and auditable tools to manage physical media. Processes and procedures ensure all media containing customer data is labeled for proper handling.

Media Protection: Media Accountability MP.L2-3.8.5

This control focuses on controlling access to media containing CUI and maintaining accountability for all such media. Customers need to define their media access and accountability policies if media exists outside of OCI. OCI operations has no access to customer content with CUI and uses rigid and auditable tools to manage physical media. Processes and procedures ensure all media containing customer data is labeled for proper handling.

Media Protection: Portable Storage Encryption MP.L2-3.8.6

This control requires implementing cryptographic mechanisms to protect CUI confidentiality on digital media during transport outside of controlled areas. OCI operations has no access to customer content with CUI and uses rigid and auditable tools to manage physical media. Processes and procedures ensure all media containing customer data is labeled for proper handling.

Media Protection: Removable Media MP.L2-3.8.7

This control involves controlling the use of removable media on system components. Customers need to define their policies regarding the use of removable media with their OCI resources if users are permitted to download or export data. While physical removable media control is primarily a customer responsibility for data removed from the cloud, OCI provides features that can support this control. Security policies can be implemented to restrict data transfer to and from cloud resources. OCI Data Safe service can be used to monitor and audit database activity, including any attempts to export data to removable media.

OCI operations has no access to customer content with CUI and uses rigid and auditable tools to manage physical media. Processes and procedures ensure all media containing customer data is labeled for proper handling.

Media Protection: Shared Media MP.L3-3.8.8

This control prohibits the use of portable storage devices if such devices have no identifiable owner.

OCI operations has no access to customer content with CUI and uses rigid and auditable tools to manage physical media. Oracle cloud does not use portable storage without an identified owner. Processes and procedures ensure all media containing customer data is labeled for proper handling.

Media Protection: Protect Backups MP.L2-3.8.9

This control focuses on protecting the confidentiality of backup CUI at storage locations. Customers need to identify their backup CUI and determine appropriate protection levels if such data is removed from their cloud environment. OCI operations has no access to customer content with CUI and uses rigid and auditable tools to manage physical media. Processes and procedures ensure all media containing customer data is labeled for proper handling.

Physical Protection: Limit Physical Access PE.L2-3.10.1

This control requires limiting physical access to organizational systems, equipment, and operating environments.

Physical access to OCI data centers is managed by Oracle and access is restricted to US citizens with proper credentials and clear business need.

Physical Protection: Monitor Facility PE.L2-3.10.2

This control involves protecting and monitoring physical facility access points. OCI data centers have 24/7 physical security with multiple layers of monitoring access control including access logs system security plans.

Physical Protection: Escort Visitors PE.L2-3.10.3

This control requires escorting visitors and monitoring their activity. Visitor escort within OCI data centers is managed by Oracle, and if visitor access is required, all activity is monitored by an appropriate escort.

Physical Protection: Physical Access Logs PE.L2-3.10.4

This control involves maintaining audit logs of physical access. OCI maintains logs of physical access to its data centers.

Physical Protection: Manage Physical Access PE.L2-3.10.5

This control requires controlling and managing physical access devices. Physical access management for OCI data centers is handled by Oracle, and all locks, keys, combinations, badges, key cards, etc. are restricted to authorized individuals and such usage is tracked and auditable.

ORACLE

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 800-171 Control	OCI technology that assists meeting the control	Core LZ deploys OCI tools that can assist meeting the control
Access Control: Authorized Access Control AC.L2-3.1.1	3.1.1	Identity and Access Management (IAM)	IAM, Object Storage, Virtual Cloud Networks
Access Control: Transaction & Function Control AC.L2-3.1.2	3.1.2	IAM	IAM, Object Storage,
Access Control: Separation of Duties AC.L2-3.1.4	3.1.4	IAM, Identity	IAM
Access Control: Least Privilege AC.L2-3.1.5	3.1.5	IAM, Identity	IAM, Object Storage,
Access Control: Unsuccessful Logon Attempts AC.L2-3.1.8	3.1.8	IAM, Identity	N/A
Access Control: Session Lock AC.L2-3.1.10	3.1.10	IAM	N/A
Access Control: Session Termination AC.L2-3.1.11	3.1.11	IAM	N/A
Access Control: Control Remote Access AC.L2-3.1.12	3.1.12	IAM, Bastions	N/A
Access Control: Remote Session Confidentiality AC.L2-3.1.13	3.1.13	IAM, Bastions	Virtual Cloud Networks
Access Control: Remote Access Routing AC.L2-3.1.14	3.1.14	Virtual Cloud Networks, Security Lists, Network Security Groups, Bastion	Virtual Cloud Networks
Access Control: Privileged Remote Access AC.L2-3.1.15	3.1.15	IAM, Cloud Guard, Network Firewall, Bastion	N/A
Access Control: External Connections AC.L2-3.1.20	3.1.20	IAM, Virtual Cloud Networks: Subnets, Route Tables, and Security Rules	Virtual Cloud Networks, Security Lists
Awareness and Training: Insider Threat Awareness AT.L2-3.2.3	3.2.3	N/A	N/A

CMMC Control	NIST SP 800-171 Control	OCI technology that assists meeting the control	Core LZ deploys OCI tools that can assist meeting the control
Audit and Accountability: System Auditing AU.L2-3.3.1	3.3.1	IAM, Logging, Audit	IAM, Cloud Guard, Object Storage
Audit and Accountability: User Accountability AU.L2-3.3.2	3.3.2	IAM, Logging, Audit	Logging
Audit and Accountability: Event Review AU.L2-3.3.3	3.3.3	Audit, Logging	N/A
Audit and Accountability: Audit Failure Alerting AU.L2-3.3.4	3.3.4	Functions, Logging, Audit	N/A
Audit and Accountability: Audit Correlation AU.L2-3.3.5	3.3.5	Functions, Logging, Audit	Topics, Cloud Guard
Audit and Accountability: Reduction and Reporting AU.L2-3.3.6	3.3.6	Audit, Logging, Log Analytics	Virtual Cloud Networks Flow Logs, Connector Hub
Audit and Accountability: Authoritative Time Source AU.L2-3.3.7	3.3.7	Audit, Logging	N/A
Audit and Accountability: Audit Protection AU.L2-3.3.8	3.3.8	IAM, Audit, Cloud Guard	N/A
Audit and Accountability: Audit Management AU.L2-3.3.9	3.3.9	IAM, Audit, Logging	Audit Logs
Configuration Management: System Baselining CM.L2-3.4.1	3.4.1	ORM	Virtual Cloud Networks, Event Rules, IAM
Configuration Management: Security Configuration Enforcement CM.L2-3.4.2	3.4.2	IAM, ORM, Cloud Guard	Virtual Cloud Networks, Event Rules, IAM

CMMC Control	NIST SP 800-171 Control	OCI technology that assists meeting the control	Core LZ deploys OCI tools that can assist meeting the control
Configuration Management: System Change Management CM.L2-3.4.3	3.4.3	IAM, Cloud Guard, Audit, Logging	Event Rule, IAM
Configuration Management: Access Restrictions for Change CM.L2-3.4.5	3.4.5	IAM, Audit, Logging,	N/A
Configuration Management: Least Functionality CM.L2-3.4.6	3.4.6	IAM, Audit, Logging, Vault	Vault, Object Storage, Event Rule, IAM
Configuration Management: Nonessential Functionality CM.L2-3.4.7	3.4.7	IAM, Cloud Guard, Security Lists, Network Security Groups, Virtual Cloud Networks	IAM, Virtual Cloud Networks, Event Rules, Network Security Group
Configuration Management: Application Execution Policy CM.L2-3.4.8	3.4.8	IAM	Virtual Cloud Networks
Configuration Management: User-Installed Software CM.L2-3.4.9	3.4.9	IAM, OS Management Hub	N/A
Identification and Authentication: Identification IA.L2-3.5.1	3.5.1	IAM, Identity	IAM
Identification and Authentication: Authentication IA-L2-3.5.2	3.5.2	IAM, Identity	IAM
Identification and Authentication: Multifactor Authentication IA.L2-3.5.3	3.5.3	IAM, Identity	IAM
Identification and Authentication: Replay-Resistant Authentication IA.L2-3.5.4	3.5.4	IAM, Identity	N/A

CMMC Control	NIST SP 800-171 Control	OCI technology that assists meeting the control	Core LZ deploys OCI tools that can assist meeting the control
Identification and Authentication: Identifier Reuse IA.L2-3.5.5	3.5.5	IAM, Identity	N/A
Identification and Authentication: Identifier Handling IA.L2-3.5.6	3.5.6	IAM/Functions	N/A
Identification and Authentication: Cryptographically Protected Passwords IA.L2-3.5.10	3.5.10	Vault, IAM	Virtual Cloud Networks, Object Storage, Vault, Compartments
Identification and Authentication: Obscure Feedback IA.L2-3.5.11	3.5.11	IAM, Identity	N/A
Incident Response: Incident Handling IR.L2-3.6.1	3.6.1	Audit, Cloud Guard, Logging, Audit	N/A
Incident Response: Incident Reporting IR.L2-3.6.2	3.6.2	Audit, Cloud Guard, logging, Audit	N/A
Maintenance: Nonlocal Maintenance MA.L2-3.7.5	3.7.5	IAM, Identity	N/A
Personnel Security: Screen Individuals PS.L2-3.9.1	3.9.1	N/A	N/A
Personnel Security: Personnel Actions PS.L2-3.9.2	3.9.2	N/A	N/A
Physical Protection: Alternative Work Sites PE.L2-3.10.6	3.10.6	Identity	N/A
Risk Assessment: Risk Assessments RA.L2-3.11.1	3.11.1	Cloud Guard, Vulnerability Scanning Service	N/A
Risk Assessment: Vulnerability Scan RA.L2-3.11.2	3.11.2	Cloud Guard, Vulnerability Scanning Service	N/A

CMMC Control	NIST SP 800-171 Control	OCI technology that assists meeting the control	Core LZ deploys OCI tools that can assist meeting the control
Risk Assessment: Vulnerability Remediation RA.L2-3.11.3	3.11.3	IAM, Cloud Guard, Vulnerability Scanning Service	IAM
Security Assessment: Security Control Assessment CA.L2-3.12.1	3.12.1	Cloud Guard, Vulnerability Scanning Service	N/A
Security Assessment: Operational Plan of Action CA.L2-3.12.2	3.12.2	Cloud Guard, Vulnerability Scanning Service	IAM
Security Assessment: Security Control Monitoring CA.L2-3.12.3	3.12.3	Cloud Guard, Vulnerability Scanning Service	N/A
Security Assessment: System Security Plan CA.L2-3.12.4	3.12.4	N/A	N/A
System and Communications Protection: Boundary Protection SC.L2-3.13.1	3.13.1	Virtual Cloud Networks, Cloud Guard, Security Zones, Network Firewall	Compartments, Security Lists, Virtual Cloud Networks, Network Security Groups, Security Lists
System and Communications Protection: Security Engineering SC.L2-3.13.2	3.13.2	Virtual Cloud Networks, Security Lists, Network Security Groups, Web Application Firewall, Firewalls	Compartments
System and Communications Protection: Role Separation SC.L2-3.13.3	3.13.3	IAM	IAM
System and Communications Protection: Shared Resource Control SC.L2-3.13.4	3.13.4	Virtual Cloud Networks, Security Lists, Network Security Groups, Web Application Firewall	N/A
System and Communications Protection: Public-Access System Separation SC.L2-3.13.5	3.13.5	Virtual Cloud Networks, Cloud Guard, Security Zones, Subnets, Service Gateway, Dynamic Routing Gateway	N/A

CMMC Control	NIST SP 800-171 Control	OCI technology that assists meeting the control	Core LZ deploys OCI tools that can assist meeting the control
System and Communications Protection: Network Communication by Exception SC.L2-3.13.6	3.13.6	IAM, Virtual Cloud Networks, Security Lists, Web Application Firewall, Network Firewall	Identity, IAM, Security List, Virtual Cloud Networks, Network Security Groups
System and Communications Protection: Data in Transit SC.L2-3.13.8	3.13.8	FastConnect, Site-2-Site VPN, IPSEC	Virtual Cloud Networks
System and Communications Protection: Connections Termination SC.L2-3.13.9	3.13.9	IAM, Bastion, LBaaS	N/A
System and Communications Protection: Key Management SC.L2-3.13.10	3.13.10	Vault	Compartments
System and Communications Protection: CUI Encryption SC.L2-3.13.11	3,13,11	Vault, FastConnect	Virtual Cloud Networks, Vault, Compartments, IAM, Object Storage
System and Communications Protection: Data at Rest SC.L2-3.13.16	3.13.16	IAM, VCN, Vault	Vault, Compartments, Object Storage, IAM,
System and Information Integrity: Flaw Remediation SI.L2-3.14.1	3.14.1	Cloud Guard, Audit	Dynamic Groups
System and Information Integrity: Malicious Code Protection SI.L2-3.14.2	3.14.2	Web Application Firewall, Cloud Guard	N/A
System and Information Integrity: Security Alerts & Advisories SI.L2-3.14.3	3.14.3	Logging, Log Analytics, Flow Logs, Cloud Guard, Notifications, Firewalls, Auditing	Virtual Cloud Networks, VCN Flow logs, Audit Logs, Service Connector Hub

CMMC Control	NIST SP 800-171 Control	OCI technology that assists meeting the control	Core LZ deploys OCI tools that can assist meeting the control
System and Information Integrity: Update Malicious Code Protection SI.L2-3.14.4	3.14.4	Web Application Firewall, Cloud Guard	N/A
System and Information Integrity: Monitor Communications for Attacks SI.L2-3.14.6	3.14.6	Virtual Cloud Networks, Security Lists, Network Security Groups, Cloud Guard, Firewalls	Firewalls, Virtual Cloud Networks, VCN Flow logs, Audit Logs, Service Connector Hub
System and Information Integrity: Identify Unauthorized Use SI.L2-3.14.7	3.14.7	IAM, Cloud Guard, Audit, Logging	Virtual Cloud Networks, VCN Flow logs, Audit Logs, Service Connector Hub, Object Storage.

CMMC 2.0 Level 2 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: Authorized Access Control AC.L2-3.1.1

The authorized access control includes different levels of access connections such as the OCI cloud administrator login, database permissions, web logins, and connections to external services. Access control in the customer's cloud environment can be simplified with a unified identity service such as Oracle Identity Domains where policies can be written to allow users access to resources within domains. The use of the Core LZ can simplify some aspects of access using Bastions and Vault. Database tools can be configured to grant access or mask data for specific users. OCI operations uses rigid and auditable identity tools to manage the control plane, conduct administration, and delivery of customer support.

The Core LZ defines the following personas that account for most organizational needs:

- IAM Administrators: manage IAM services and resources including compartments, groups, dynamic groups, policies, identity providers, authentication policies, network sources, tag defaults. However, this group is not allowed to manage the out-of-box Administrators and Credential Administrators groups or modify the out-of-box Tenancy Admin policy.
- Credential Administrators: manage users capabilities and users credentials in general, including API keys, authentication tokens and secret keys.
- Cost Administrators: manage budgets and usage reports.
- Auditors: entitled with read-only access across the tenancy and the ability to use cloud-shell to run the cis_reports.py script.

- Announcement Readers: for reading announcements displayed in OCI Console.
- Security Administrators: manage security services and resources including Vaults, Keys, Logging, Vulnerability Scanning, Web Application Firewall, Bastion, Service Connector Hub.
- Network Administrators: manage OCI network family, including VCNs, Load Balancers, DRGs, VNICs, IP addresses.
- Application Administrators: manage application related resources including Compute images, OCI Functions, Kubernetes clusters, Streams, Object Storage, Block Storage, File Storage.
- Database Administrators: manage database services, including Oracle VMDB (Virtual Machine), BMDB (Bare Metal), ADB (Autonomous databases), Exadata databases, MySQL, NoSQL, etc.
- ExaCS Administrators (only created when ExaCS compartment is created): manage Exadata infrastructure and VM clusters in the ExaCS compartment.
- Storage Administrators: the only group allowed to delete storage resources, including buckets, volumes, and files. Used as a protection measure against inadvertent deletion of storage resources.

The Core LZ also deploys an optional Object Storage bucket(s) in the AppDev Compartment. Those bucket(s) are deployed as a private bucket.

The Core LZ changes authentication settings but does not create OCI IAM users, API Keys of users, secrets of users, auth tokens of users, or Database Passwords of users. The Core LZ also does not deploy any Compute instance. The Core LZ deploys VCNs that can be used for deploying Compute instances, and the Secure Workload Module deploys Compute instances with Secure Boot enabled.

Access Control: Transaction & Function Control AC.L.-3.1.2

The transaction and function control gives guidance about roles and permissions, including Role Based Access Controls (RBAC) for groups, individuals, or systems. It is designed to allow authorized users access to the data needed to complete their designated work. This control applies to access provided to the OCI administrator console Platform as a Service (PaaS) like Database or Integrations Cloud, and applications installed in hosts on Infrastructure as a Service (IaaS) such as web servers. OCI operations uses rigid and auditable Identity tools to manage the control plane, conduct administration, and delivery of customer support. Access is provided using a least privilege model.

Oracle Data Safe assesses the security of the customer's database users and helps find risks. It evaluates user types, how users authenticate, password policies assigned to each user, and how long it has been since each user has changed their password. Data Safe includes a direct link to audit records related to each user to help the customer deploy security controls and policies. With Identity Domains, the customer can define roles and assign these roles to various users performing specific work. For example, the customer may assign the application administrator role for a user they want to manage applications.

The Core LZ defines the following personas that account for most organizational needs:

- IAM Administrators: manage IAM services and resources including compartments, groups, dynamic groups, policies, identity providers, authentication policies, network sources, tag defaults. However, this group is not allowed to manage the out-of-box Administrators and Credential Administrators groups or modify the out-of-box Tenancy Admin policy.
- Credential Administrators: manage users capabilities and users credentials in general, including API keys, authentication tokens and secret keys.

- Cost Administrators: manage budgets and usage reports.
- Auditors: entitled with read-only access across the tenancy and the ability to use cloud-shell to run the cis_reports.py script.
- Announcement Readers: for reading announcements displayed in OCI Console.
- Security Administrators: manage security services and resources including Vaults, Keys, Logging, Vulnerability Scanning, Web Application Firewall, Bastion, Service Connector Hub.
- Network Administrators: manage OCI network family, including VCNs, Load Balancers, DRGs, VNICs, IP addresses.
- Application Administrators: manage application related resources including Compute images, OCI Functions, Kubernetes clusters, Streams, Object Storage, Block Storage, File Storage.
- Database Administrators: manage database services, including Oracle VMDB (Virtual Machine), BMDB (Bare Metal), ADB (Autonomous databases), Exadata databases, MySQL, NoSQL, etc.
- ExaCS Administrators (only created when ExaCS compartment is created): manage Exadata infrastructure and VM clusters in the ExaCS compartment.
- Storage Administrators: the only group allowed to delete storage resources, including buckets, volumes, and files. Used as a protection measure against inadvertent deletion of storage resources.

The Core LZ also deploys an optional Object Storage bucket(s) in the AppDev Compartment. Those bucket(s) are deployed as a private bucket.

The Core LZ changes authentication settings but does not create OCI IAM users, API Keys of users, secrets of users, auth tokens of users, or database passwords of users. The Core LZ also does not deploy any Compute instance. The Core LZ deploys 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.

Finally, the Core LZ restricts OCI IAM policies for the Network Admins, Security Admins, App Admin, and Database Admins groups which allows them to create storage services but prevents them from deleting storage services. The Core LZ also creates a Storage Admin policy and group which allows the deletion of storage resources but not their creation.

Access Control: Separation of Duties AC.L2-3.1.4

This control is designed to limit the control of any one individual and the intentional compromise of data or service. Examples of such separation could include different administrators for database and networking security. OCI can achieve access control separation of duty by implementing IAM. Customers can use compartments to isolate their resources to achieve greater security and control. OCI operations uses rigid and auditable identity tools to manage the control plane, conduct administration, and delivery of customer support. Access is granted with separation of duty as a priority.

The Core LZ restricts adds where conditions to the OCI IAM policies for the Network Admins, Security Admins, App Admin, and Database Admins groups which allows them to create storage services but prevents them from deleting storage services. The Core LZ also creates a Storage Admin policy and group, which allows the deletion of storage resources but not their creation.

Access Control: Least Privilege AC.L2-3.1.5

This control is designed to grant access and rights to users and process with only the capabilities to complete the tasks required. The intent of the control is to prevent users from conducting activities that are outside of their designated role. Customers can achieve least privilege access by implementing Identity and Access Management. Customers can use IAM to limit access via roles, policies, and user groups. OCI operations uses rigid and auditable identity tools to manage the control plane, conduct administration, and delivery of customer support. Access is provided using a least privilege model.

The Core LZ defines the following personas that account for most organizational needs:

- IAM Administrators: manage IAM services and resources including compartments, groups, dynamic groups, policies, identity providers, authentication policies, network sources, tag defaults. However, this group is not allowed to manage the out-of-box Administrators and Credential Administrators groups. It is also not allowed to modify the out-of-box Tenancy Admin policy.
- Credential Administrators: manage users capabilities and users credentials in general, including API keys, authentication tokens and secret keys.
- Cost Administrators: manage budgets and usage reports.
- Auditors: entitled with read-only access across the tenancy and the ability to use cloud-shell to run the cis_reports.py script.
- Announcement Readers: for reading announcements displayed in OCI Console.
- Security Administrators: manage security services and resources including Vaults, Keys, Logging, Vulnerability Scanning, Web Application Firewall, Bastion, Service Connector Hub.
- Network Administrators: manage OCI network family, including VCNs, Load Balancers, DRGs, VNICs, IP addresses.
- Application Administrators: manage application related resources including Compute images, OCI Functions, Kubernetes clusters, Streams, Object Storage, Block Storage, File Storage.
- Database Administrators: manage database services, including Oracle VMDB (Virtual Machine), BMDB (Bare Metal), ADB (Autonomous databases), Exadata databases, MySQL, NoSQL, etc.
- ExaCS Administrators (only created when ExaCS compartment is created): manage Exadata infrastructure and VM clusters in the ExaCS compartment.
- Storage Administrators: the only group allowed to delete storage resources, including buckets, volumes, and files. Used as a protection measure against inadvertent deletion of storage resources.

The Core LZ also deploys an optional Object Storage bucket(s) in the AppDev Compartment. Those bucket(s) are deployed as a private bucket.

The Core LZ modifies existing users and defines the following personas that account for most organizational needs:

- IAM Administrators: manage IAM services and resources including compartments, groups, dynamic groups, policies, identity providers, authentication policies, network sources, tag defaults. However, this group is not allowed to manage the out-of-box Administrators and Credential Administrators groups or modify the out-of-box Tenancy Admin policy.

- Credential Administrators: manage users capabilities and users credentials in general, including API keys, authentication tokens and secret keys.

The Core LZ restricts with where conditions in the OCI IAM policies for the Network Admins, Security Admins, App Admin, and Database Admins groups, which allows them to create storage services but prevents them from deleting storage services. The Core LZ also creates a Storage Admin policy and group, which allows the deletion of storage resources but not their creation.

Access Control: Unsuccessful Logon Attempts AC.L2-3.1.8

This control is designed to prevent unauthorized access to resources with the assumption that consecutive failed login attempts may indicate inappropriate or malicious activity. Access lockout can be released after a designated period of time. Identity and Access management has a mechanism for limiting the number of incorrect logins for customers. Users will need to reset their passwords after the configurable number of incorrect login attempts. OCI operations limits the number of failed access attempts for all activities associated with managing the control plane, conducting administration, and delivery of customer support.

Access Control: Session Lock AC.L2-3.1.10

This control is intended to minimize the risk of unauthorized access to resources when an authorized user leaves the vicinity of the system during an active session. All US Government Cloud OCI consoles log out users after 15 minutes of inactivity. Customers can use Identity cloud services to manage session settings for other users and services. OCI operations locks idle sessions for all activities associated with managing the control plane, conducting administration, and delivery of customer support.

Access Control: Session Termination AC.L2-3.1.11

This control is intended to minimize the risk of unauthorized access to resources by terminating authorized user access after a defined condition, such as a specified time of day, a specified activity, or after a period of inactivity. All US Government Cloud OCI consoles will log out users after 15 minutes of inactivity. Customers can use Identity cloud services to manage session settings for other users and services. OCI can limit access and sessions for all activities associated with managing the control plane, conducting administration, and delivery of customer support.

Access Control: Control Remote Access AC.L2-3.1.12

This control is designed to manage users' remote access to the system when connecting via a broad variety of remote network methods. This control logs and audits connection activities to monitor remote access sessions. Bastion service can allow customers to connect to Compute instances in OCI and gain control. Administrators can restrict certain ports needed to connect remotely. OCI monitors and limits access and sessions for all activities associated with managing the control plane, conducting administration, and delivery of customer support using Bastions, VPN, tokens, and other operational tools.

Access Control: Remote Access Confidentiality AC.L2-3.1.13

This control requires the use of a FIPS 140-1 or -2 validated module to encrypt information that is exchanged through a remote connection. OCI offers several features and services that help meet session encryption including SSH for encrypted terminal connection, VPNs for secure encrypted connectivity, IAM for allowing granular control, and Logging and Monitoring for providing visibility into remote access activities. All remote access and sessions for all activities associated with managing the control plane, conducting administration, and delivery of customer support are conducted using validated FIPS 140-2 cryptography.

The Core LZ does not deploy any Compute instance. The Core LZ deploys VCNs that can be used for deploying Compute instances, and the Secure Workload Module deploys Compute instances with in-transit encryption enabled.

Access Control: Remote Access Routing AC.L2-3.1.14

In an effort to reduce unauthorized access to systems and data, this control is intended to route access to the minimum number of points required. OCI's Bastion service that allows users to connect to Compute instances in OCI and gain control. Administrators can restrict certain ports needed to connect remotely. All remote access is restricted for managing the control plane, conducting administration, and delivery of customer support.

The Core LZ 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; however, the application servers and database servers are always created as private. Route rules and network security rules are configured based on provided connectivity settings. The Core LZ can be deployed to deploy network security devices like 3rd 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: https://docs.oracle.com/en/solutions/deploy-partners-to-cis-lz/index.html.

Access Control: Privileged Remote Access AC.L2-3.1.15

This control seeks to limit critical operations to only those users with the appropriate authorization, including commands that would grant access to security-related data or that could impact the stability or integrity of the system as a whole. OCI customers can restrict remote access to Oracle US Government Cloud infrastructure using OCI network firewall, which limits remote access to Oracle US Government Cloud Bastion host connections. All other connections are denied by default. For OCI operations, privileged control and access is restricted for managing the control plane, conducting administration, and delivery of customer support.

The Core LZ does not create or modify OCI IAM users.

Access Control: External Connections AC.L2-3.1.20

The external connections control is a broad category that includes connections within the OCI cloud administrator console, databases, applications, web services, APIs, on-premises systems, or multi-cloud systems. The primary purpose of the Core LZ is to create secured external connections and isolated VCN architecture, which can help address these controls. For OCI operations, external connections are limited and monitored in the management of the control plane, conducting administration, and delivery of customer support.

The Core LZ includes several native cloud services and features to meet external connections controls. OCI's Network Firewall is a next-generation managed network firewall and intrusion detection and prevention service for the customer's Oracle Cloud Infrastructure VCN. OCI Network Firewall service offers simple setup and deployment that gives the customer visibility into traffic entering their cloud environment as well as traffic between subnets. Our Web Application Firewall (WAF) service protects applications from malicious and unwanted internet traffic. WAF can protect any internet facing endpoint with consistent rule enforcement across the customer's application. Our Connector Hub is a cloud message bus platform that offers a single pane of glass for describing, executing, and monitoring interactions when moving data between OCI services. OCI Cloud Guard service helps the customer monitor, identify, achieve, and maintain a strong security posture on Oracle Cloud. If Cloud Guard detects malicious data, it takes corrective actions based on the customer's configuration.

The Core LZ does not create OCI IAM users or API Keys of users. The Core LZ creates a security list for each VCN it creates. The security list only allows port 22 connections from on-premises CIDRs or the hub network. The on-premises Classless Inter-Domain Routing (CIDRs) variable does not allow 0.0.0.0/0. The Landing Zone deploys a Bastion network security group (NSG) for each VCN it creates. That NSG allows port 22; however, the variable for ingress CIDRs does not allow 0.0.0.0/0. That NSG allows 3389; however, the variable for ingress CIDRs does not allow 0.0.0.0/0.

The Core LZ does not deploy any Oracle Integration Cloud instances. The Core LZ does not deploy any Oracle Analytics Cloud (OAC) instances. The Core LZ deploys VCNs with app subnets, which are private, that can be used for deploying OAC instances. The Core LZ does not deploy any Autonomous Shared Databases (ADB-S). The Core LZ deploys VCNs with database subnets, which are private, that can be used for deploying an ADB-S.

Awareness and Training: Insider Threat Awareness AT.L2-3.2.3

This control is designed to inform and educate all users who interact with a system about the different types of insider threats and how to minimize exposure. Customers are responsible for implementing this control and providing training to their staff and users. OCI operations conducts annual training and testing of knowledge for all staff who could interact with cloud operations.

Audit and Accountability: System Auditing AU.L2-3.3.1

This control details the need to capture logs of unlawful or unauthorized activity within the system and retain those logs for evaluation. The logs should include sufficient detail to identify who, when, what, and where for these activities. OCI Auditing and Logging services help customers create, retain, and analyze audit logs. Customers can configure retention policies to ensure adequate retention logs. For OCI operations, logs are captured and evaluated with a SIEM and retained for the management of the control plane, conducting administration, and delivery of customer support.

The Core LZ creates at least two topics each with a subscription. The two default topics are:

- Security Topic and subscription, which is where all IAM related events are sent.
- Network Topic and subscription, which is where all network related events are sent.

The Core LZ enables VCN flow logs for all subnets it deploys. The Core LZ enables OCI Cloud Guard with all the detectors and responders at the root compartment. The Core LZ creates an OCI event rules for Cloud Guard events. The Core LZ deploys an optional Object Storage bucket(s) in the AppDev Compartment. Those bucket(s) are deployed and write logging is enabled.

Audit and Accountability: User Accountability AU.L2-3.3.2

This control is designed to relate an activity to a user through the use of logs and then retain the records of this activity for access, usage, connectivity, maintenance, and physical access. For the customer portion of this control, OCI Audit service can be used to assist in auditing and tracing. For OCI operations, logs are captured for all user activity and retained for auditing in the management of the control plane, conducting administration, and delivery of customer support.

The Core LZ will aggregate OCI service logs to be used in third-party SIEMs. The architecture is designed to collect, centralize, and aggregate various logs such as OCI Audit logs, service logs, and security events.

Audit and Accountability: Event Review AU.L2-3.3.3

This control is designed to review and re-evaluate the policies for the use of logs and record retention over time to ensure the appropriate safeguards are achieved as changes to the systems as a whole occur over time. OCI customers are responsible for alerting organization-defined personnel or roles in the event of an audit processing failure. For OCI operations, auditing, logging,

record retention policies are reviewed on a regular basis in the management of the control plane, conducting administration, and delivery of customer support.

Audit and Accountability: Audit Failure Alerting AU.L2-3.3.4

This control requires an alert be generated when any audit logging process fails anywhere in the system, hardware, or software. OCI customers are responsible for responding to failed audit log alerts that are generated by OCI and ensure services hosted in OCI adhere to the same policy. For OCI operations, auditing log failures generate alerts for the management of the control plane, conducting administration, and delivery of customer support.

Audit and Accountability: Audit Correlation AU.L2-3.3.5

This control seeks to correlate audit record review, analysis, and reporting processes so they can be investigated and generate a response to evidence of unlawful, unauthorized, suspicious, or unusual activity. OCI customers are responsible for correlating audits for investigation and must implement proper log retention. For OCI operations, anomalous activity captured in logs and audited is investigated and acted upon for the management of the control plane, conducting administration, and delivery of customer support.

The Core LZ creates at least two topics each with a subscription. The two default topics are:

- Security Topic and subscription, which is where all IAM related events are sent.
- Network Topic and subscription, which is where all network related events are sent.

The Core LZ creates an OCI event rule for Cloud Guard events.

Audit and Accountability: Reduction & Reporting AU.L2-3.3.6

This control is designed to reduce the total record volume by organizing raw log/audit data across disparate systems and preparing it for analysis and review in a consolidated and filtered format. OCI customers are responsible for providing an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents. For OCI operations, audit logs are analyzed, filtered, and organized for analyst review for the management of the control plane, conducting administration, and delivery of customer support.

The Core LZ channels VCN flow logs and Audit logs through Service Connector Hub (SCH) to Object Storage (by default), thus providing a consolidated view of logging data and making it more easily consumable by customers' SIEM and SOAR systems.

Audit and Accountability: Authoritative Time Source AU.L2-3.3.7

This control is designed to use a standardized method of generating time stamps, typically Coordinated Universal Time (UTC), with an appropriate granularity and synchronization across components in the system. OCI's virtual machine instances and other cloud resources are configured to synchronize their system clocks with an authoritative time source such as NTP. By default, OCI Audit event-related dates and times use the UTC format: YYYY-MM-DDThh:mm:ss.mscZ. For example, 2022-03-24T10:24:24.022Z. For OCI operations, UTC and an NTP time source are used for the management of the control plane, conducting administration, and delivery of customer support.

Audit and Accountability: Audit Protection AU.L2-3.3.8

This control seeks to limit access to audit logs and audit tools to only users who require access and to ensure the audit logs and audit tools cannot be deleted or modified. IAM can be used to protect audit logs. Customers can create policies to limit who can access, view, and modify audit logs. For

OCI operations, audit logging and audit tools have the proper protections and access policies for the management of the control plane, conducting administration, and delivery of customer support.

The Core LZ audit logs are stored in Object Storage, which is encrypted with CMK. Audit logs are read-only and not modifiable.

Audit and Accountability: Audit Management AU.L2-3.3.9

This control seeks to limit access to audit logs and audit tools to a privileged set of users. These privileged users are separate from the users whose access is logged and audited to avoid creating a conflict of interest. IAM can be used to protect audit logs. Customers can create policies to limit who can access, view, and modify audit logs. For OCI operations, audit logging and audit tools have the proper access policies to privileged users for the management of the control plane, conducting administration, and delivery of customer support.

The Core LZ configures audit logs so that only Virtual Data Center Managed Services (VDMS) admins have access to audit logs.

Configuration Management: System Baselining CM.L2-3.4.1

This control seeks to establish and maintain a baseline for the system, its components, networks, software (including licenses), hardware, connections, network addresses, component names/types/serial numbers, and locations. The baseline should be documented and reviewed regularly across all applicable owners and organizations. OCI Resource Manager allows customers to define and create resources using Infrastructure as Code. These templates are reusable and can be version controlled. For OCI operations, the control plane, and the services in OCI cloud have rigorous configuration management tools and processes to establish and maintain a configuration baseline for the control plane, conducting administration, and delivery of customer support.

The Core LZ changes authentication settings but does not create OCI IAM users, API Keys of users, secrets of users, auth tokens of users, or Database Passwords of users. The Core LZ also does not deploy any Compute instance. The Core LZ deploys VCNs that can be used for deploying Compute instances, and the Secure Workload Module deploys Compute instances with Secure Boot enabled. The Core LZ deploys VCNs that can be used for deploying Compute instances, and the Secure Workload Module deploys Compute instances with in-transit encryption enabled.

The Core LZ creates an OCI event rule for Identity Provider changes, IDP mapping changes, IAM group changes, IAM policy changes, IAM user changes, VCN changes, network route table changes, network security group changes, and network gateway changes.

Configuration Management: Security Configuration Enforcement CM.L2-3.4.2

This control seeks to establish and enforce security settings for the system, its components, network gear, software, hardware, input devices, and security parameters, including account setting permissions, ports, protocols, and connections. IAM can be used to protect audit logs by managing access. Customers can create policies to limit who can access, view, and modify audit logs. For OCI operations, the infrastructure and management tools policies and processes to establish enforce security settings for the control plane, conducting administration, and delivery of customer support.

The Core LZ changes authentication settings but does not create OCI IAM users, API Keys of users, secrets of users, auth tokens of users, or Database Passwords of users. The Core LZ also does not deploy any Compute instance. The Core LZ deploys VCNs that can be used for deploying Compute instances, and the Secure Workload Module deploys Compute instances with Secure Boot enabled. The Core LZ deploys VCNs that can be used for deploying Compute instances, and the Secure Workload Module deploys Compute instances with in-transit encryption enabled.

The Core LZ creates an OCI event rule for Identity Provider changes, IDP mapping changes, IAM group changes, IAM policy changes, IAM user changes, VCN changes, network route table changes, network security group changes, and network gateway changes.

Configuration Management: System Change Management CM.L2-3.4.3

This control is designed to implement configuration change control by tracking, reviewing, approving, and logging changes. These changes include upgrades and modifications to systems, and software, through control or advisory boards. All such changes (even unscheduled or unauthorized) should be logged and reviewed. IAM can be used to protect audit logs. Customers can create policies to limit who can access, view, and modify audit logs. For OCI operations, Oracle enforces rigorous change management procedures and policies, logs all activities, and reviews configuration outcomes for the control plane, conducting administration, and delivery of customer support.

The Core LZ creates an OCI event rule for Identity Provider changes, IDP mapping changes, IAM group changes, IAM policy changes, IAM User changes, VCN changes, network route table changes, network security group changes, and network gateway changes.

Configuration Management: Access Restrictions for Change CM.L2-3.4.5

This control restricts the ability to make changes to hardware, software, or firmware that can impact the security of the system. Only qualified and authorized individuals should have access to the physical hardware, software, workflows, external interfaces, and change schedules. IAM can be used to restrict changes based on users, role, groups, etc. For OCI operations, access and control is strictly limited to trained and authorized users for any changes impacting the control plane, conducting administration, and delivery of customer support.

The Core LZ configures logical access to be defined based on administrative groups and changes to privileged access are logged.

Configuration Management: Least Functionality CM.L2-3.4.6

This control limits user access to only the capabilities required to complete a user's assigned task(s). Not all users need access to all systems, tools, or actions in the completion of their assigned role. This control can be satisfied by limiting access and employing least privilege as part of the comprehensive IAM policy. OCI operations uses least privilege for access to the control plane, conducting administration, and delivery of customer support.

The Core LZ deploys an optional (Level 2 selected) OCI Vault in the Security Compartment and generates an optional CMK. It also deploys required OCI IAM policies for the Object Storage service and OCI IAM groups to use CMKs in the Security Compartment. The Core LZ deploys an optional Object Storage bucket in the AppDev Compartment. That bucket is deployed with versioning enabled. It also deploys required OCI IAM policies for the Block Volume service and OCI IAM groups to use CMKs in the Security Compartment. It also deploys required OCI IAM policies for the FSS and OCI IAM groups to use keys in the Security Compartment.

The Core LZ changes authentication settings but does not create OCI IAM users, API Keys of users, secrets of users, auth tokens of users, or Database Passwords of users. The Core LZ also does not deploy any Compute instance. The Core LZ deploys VCNs that can be used for deploying Compute instances, and the Secure Workload Module deploys Compute instances with Secure Boot enabled. The Core LZ deploys VCNs that can be used for deploying Compute instances, and the Secure Workload Module deploys Compute instances with in-transit encryption enabled.

The Core LZ creates an OCI event rule for Identity Provider changes, IDP mapping changes, IAM group changes, IAM policy changes, IAM user changes, VCN changes, network route table changes, network security group changes, and network gateway changes.

Configuration Management: Nonessential Functionality CM.L2-3.4.7

This control is designed to limit the use of non-essential software, restrict the use of port and protocols, and limit the roles that can approve or execute simultaneous actions within the system. This control can be satisfied by limiting access and employing least privilege as part of the comprehensive IAM policy. For OCI operations, Oracle enforces least privilege and has policies to evaluate the need of software and approve the addition of software for the control plane, conducting administration, and delivery of customer support.

The Core LZ changes authentication settings but does not create OCI IAM users, API Keys of users, secrets of users, auth tokens of users, or Database Passwords of users. The Core LZ also does not deploy any Compute instance. The Core LZ deploys VCNs that can be used for deploying Compute instances and the Secure Workload Module deploys Compute Instances with Secure Boot enabled. The Core LZ deploys VCNs which can be used for deploying Compute instances and the Secure Workload Module deploys Compute instances with in-transit encryption enabled.

The Core LZ creates an OCI event rule for Identity Provider changes, IDP mapping changes, IAM group changes, IAM policy changes, IAM user changes, VCN changes, network route table changes, network security group changes, and network gateway changes.

The Core LZ does not create OCI IAM users or API Keys of users. The Core LZ creates 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. The security list 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. The Core LZ deploys a Bastion network security groups (NSG) for each VCN it creates. That NSG allows 22; however, the variable for ingress CIDRs does not allow 0.0.0.0/0. That NSG allows 3389; however, the variable for ingress CIDRs does not allow 0.0.0.0/0. The Core LZ does not deploy any Oracle Integration Cloud instances. The Core LZ does not deploy any OAC instances. The Core LZ deploys VCNs with app subnets, which are private, that can be used for deploying OAC instances. The Core LZ does not deploy any ADB-S. The Core LZ deploys VCNs with database subnets which are private that can be used for deploying an ADB-S.

The Core LZ does not deploy any Compute instance. The Core LZ deploys VCNs that can be used for deploying Compute instances, and the Secure Workload Module deploys Compute instances with the Legacy Metadata service endpoint disabled.

Configuration Management: Application Execution Policy CM.L2-3.4.8

This control seeks to evaluate the software used in the system by leveraging blacklisting and whitelisting (preferred) to limit software usage. OCI operations leverages both blacklisting and whitelisting (primary) and evaluates software on a regular basis for the control plane, conducting administration, and delivery of customer support.

The Core LZ does not deploy any Compute instance. The Core LZ deploys VCNs that can be used for deploying Compute instances, and the Secure Workload Module deploys Compute instances with the Legacy Metadata service endpoint disabled.

Configuration Management: User-Installed Software CM.L2-3.4.9

This control seeks to manage users who are authorized to install software in the delivery of a solution using privileges or policy by establishing approved/prohibited software lists through procedural and/or automated methods. Customers need to create policies and evaluate the software they deploy within a cloud tenancy. OCI operations evaluates and limits what software and which users can install software for the control plane, conducting administration, and delivery of customer support.

Identification and Authentication: Identification IA.L2-3.5.1

The identification control applies to users, systems, and processes that may need to access sensitive data. This can be as simple as the administrator's username for the OCI console. Oracle offers a centralized Identity Management service for those accessing data through the solution the customer has built on OCI, applications, and web front-ends. In addition, Oracle Data Safe can minimize user risk by managing privileges and authentications. It can identify risky behavior and overprivileged users. Data Safe identifies which users present the highest risk, reviews privileges granted to those users, and allows for analysis of user activity. This allows the customer to evaluate profile information such as user type, password policies, last login, and password age. OCI operations uses identity management tool for identity to access the control plane, conducting administration, and delivery of customer support.

The Core LZ leverages IAM as the primary method of identification.

Identification and Authentication: Authentication IA-L2-3.5.2

The authentication control requires verifying that the identity is who they claim to be. OCI administrators may control this through a password and multifactor authentication process. Organizations should set policy for minimum password length, validation window, number of allowed rejections including biometric authentication. A similar process may be used with our Identity Management tool that associates one or more authentication steps as part of verifying an identity. The Core LZ implements Identity Domains by default and includes support for x509 authentication that the customer must configure as soon as it is deployed. Security Advisor is available to simplify the authentication of specific users with customer managed encryption keys to limit resource access without creating more policies. Oracle Database provides authentication controls to manage who has access to the database and users can be centrally managed in OCI Identity and Access Management (IAM). An Oracle Database administrator works with an OCI IAM administrator to manage the authentication and authorization of OCI IAM users who need to connect to the Oracle Database as a Service (DBaaS) instance. The Oracle DbaaS instances that IAM users can connect to are Oracle Autonomous Database on Shared Exadata Infrastructure, Oracle Autonomous Database on Dedicated Exadata Infrastructure, and Oracle Base Database Service. OCI operations uses identity management tools (including token and multifactor) to authenticate access the control plane, conducting administration, and delivery of customer support.

The Core LZ leverages IAM as the primary method of authentication.

Identification and Authentication: Multifactor Authentication IA.L2-3.5.3

This control details the use of multifactor authentication including the use of more than one of the following: password, PIN, token/cryptographic device, or biometric characteristic. Multifactor authentication can be used at multiple layers of access and can include local or network access and can use VPN outside of organization-controlled endpoints. OCI operations uses identity management tools (including token and multifactor) to authenticate access the control plane, conducting administration, and delivery of customer support.

The Core LZ leverages IAM, but does not create or modify OCI IAM users.

Identification and Authentication: Replay-Resistant Authentication IA.L2-3.5.4

This control is designed to resist replay attacks by preventing recorded or the replay of a previous authentication. It is recommended to follow IAM best practices in configuring authentication. OCI operations uses identity management tools and follows best-practices for authentication to access the control plane, conducting administration, and delivery of customer support.

Identification and Authentication: Identifier Reuse IA.L2-3.5.5

This control is designed to prevent a previously used identifier from being reused to identify a new user, group, role, or device. Oracle IAM can help with the prevention of identifiers by permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. For OCI operations, Oracle uses identity management tools and prevents reuse of identifiers to access the control plane, conducting administration, and delivery of customer support.

Identification and Authentication: Identifier Handling IA.L2-3.5.6

This control is designed to disable an identifier for a user, group, role, or device that is no longer active to prevent unauthorized access through an inactive account. Oracle IAM can help with the management of inactive identifiers by password policy. OCI operations uses identity management tools and disable inactive identifiers to access the control plane, conducting administration, and delivery of customer support.

Identification and Authentication: Cryptographically Protected Passwords IA.L2-3.5.10

This control requires passwords to be cryptographically protected when stored and transmitted. Customers can use Oracle Identity and vault tools to provide password encryption. OCI operations uses identity management and key management tools that use encryption for storage and transmission of passwords to access the control plane, conducting administration, and delivery of customer support.

The Core LZ does not deploy any Compute instance. The Core LZ deploys VCNs that can be used for deploying Compute instances, and the Secure Workload Module deploys Compute instances with in-transit encryption enabled.

The Core LZ deploys an optional (Level 2 selected) OCI Vault in the Security Compartment and generates an optional CMK. It also deploys required OCI IAM policies for the Object Storage service and OCI IAM groups to use CMKs in the Security Compartment. The Core LZ deploy an optional Object Storage bucket in the AppDev Compartment. That bucket is deployed is deployed with versioning enabled. The Core LZ deploys an optional (Level 2 selected) OCI Vault in the Security Compartment and generates an optional CMK. It also deploys required OCI IAM policies for the Block Volume service and OCI IAM groups to use CMKs in the Security Compartment. It also deploys required OCI IAM policies for the Block Volume service and OCI IAM groups to use CMKs in the Security Compartment. It also deploys required OCI IAM policies for the FSS and OCI IAM groups to use keys in the Security Compartment.

Identification and Authentication: Obscure Feedback IA.L2-3.5.11

This control requires that feedback, as part of authentication, does not expose data that could be used to allow unauthorized access, such as obscuring password characters exposed in the UI during authentication. Customers can use Oracle Identity tools to limit authentication feedback. OCI operations uses identity management and key management tools that restrict feedback of passwords to access the control plane, conducting administration, and delivery of customer support.

Incident Response: Incident Handling IR.L2-3.6.1

This control details numerous aspects of incident response. Incident response includes initial design and definition of the process and system (including supply chain), auditing and logging, employee training, and cross organization communication both physical and logical. Customers need to design and manage this process for the implementation of service within their tenancy. OCI operations uses rigorous tools, policies, and procedures to manage incident response for the control plane, conducting administration, and delivery of customer support.

Incident Response: Incident Reporting IR.L2-3.6.2

This control requires tracking and documenting security incidents, including maintaining records, status, and additional information about the incident such as forensics, trends, and handling. Incident information can come from reports, logs, response teams, network and physical access monitoring, and user reports. Both actual and suspected incidents should be tracked, and certain security incidents require timely reporting to authorities as reflected by applicable laws. Customers need to design and manage this process for responding to incidents within their tenancy. OCI operations uses tools, policies, and procedures to manage and track incident response for the control plane, conducting administration, and delivery of customer support.

Maintenance: Nonlocal Maintenance MA.L2-3.7.5

This control requires that all nonlocal maintenance and diagnostic work be completed in accordance with control IA.L2-3.5.3, which instructs that nonlocal access also uses multifactor authentication. Customers can leverage OCI identity tools that include multifactor authentication for non-local access. OCI operations uses multifactor authentication for nonlocal access for the control plane, conducting administration, and delivery of customer support.

Personnel Security: Screen Individuals PS.L2-3.9.1

This control requires all individuals with access to CUI data be vetted to evaluate/assess the individuals conduct, integrity, judgement, loyalty, and stability prior to granting such access. This screening should reflect applicable laws, directives, orders, regulations, policies, and criteria appropriate for assigned access. Customers must screen employees in accordance with the expectations of the control. OCI operations does not have access to customer content with CUI.

Personnel Security: Personnel Actions PS.L2-3.9.2

This control requires all individuals with access to CUI data be interviewed through an exit interview to ensure they continue to protect any CUI data they have been exposed to. The individuals must also return all equipment (including manuals, tokens, building passes) that may have been used in accessing CUI data. Extra care must be taken for any individuals who have been or will be terminated for cause to ensure the integrity of the CUI. Customers should conduct exit interviews of departing employees in accordance with the expectations of the control and ensure all appropriate equipment be returned, and manage terminations appropriately. OCI operations does not have access to customer content with CUI.

Physical Protection: Alternative Work Sites PE.L2-3.10.6

This control requires all individuals with access to CUI data at an alternate worksite (government office, private residence, etc.) ensure that CUI access and data protection remain in place. Customers should train employees and use the same access techniques for remote sites as are in place for traditional work locations. OCI operations does not have access to customer content with CUI.

Risk Assessment: Risk Assessments RA.L2-3.11.1

This control is designed periodically assess risks to the system boundary. This review should cross all organizations that have the ability to impact they system including individuals, assets, operations both internal and external. To meet this control, customers should create set a schedule for such periodic reviews. OCI operations enforces formal review processes, both scheduled and ad hoc as needed, to assess access risk for the control plane, conducting administration, and delivery of customer support.

Risk Assessment: Vulnerability Scan RA.L2-3.11.2

This control is designed to periodically conduct vulnerability scans of the environment. The scans should be updated to include newly identified vulnerabilities and hardware, software, ports, protocols, patches, and flows. It is recommended to use tools that are Security Content Automated Protocol (SCAP) validated, express vulnerabilities in with Common Vulnerabilities and Exposure (CVE) naming and Common Vulnerability Scoring System (CVSS), employ Open Vulnerability Assessment Language (OVAL), and use sources such as Common Weakness Enumeration (CWE), and National Vulnerability Database (NVD). This control should be conducted only by users with the proper privileged access. To meet this control, customers should create set a schedule for vulnerability scans consistent with the expectations of the control. OCI operations enforces prescriptive and regular vulnerability scans for the holistic cloud environment including the control plane.

Risk Assessment: Vulnerability Remediation RA.L2-3.11.3

This control is designed to ensure the vulnerabilities discovered in RA.L2-3-11.2 are remediated. The level of risk of vulnerabilities should influence the prioritization and effort expended in the remediation. To meet this control, customers should remediate vulnerabilities consistent with the expectations of the control. OCI operations has tools to manage and prioritize the remediation of vulnerabilities for the management of the control plane, conducting administration, and delivery of customer support.

The Core LZ defines a dynamic group for the Compute Agent to be used by the Compute management agent in the AppDev compartment, which supports the deployment of OS Management.

Security Assessment: Security Control Assessment CA.L2-3.12.1

This control requires that the security assessment is periodically reviewed as part of the system development lifecycle to ensure the proper safeguards and countermeasures are in place. Security assessment reports should be complete, accurate and current to enable risk-based decisions, ensure compliance, and address vulnerabilities. To meet this control, customers should document their security posture and periodically review the security assessment consistent with the expectations of the control. OCI operations reviews the security posture of the control plane, conducting administration, and delivery of customer support.

Security Assessment: Operational Plan of Action CA.L2-3.12.2

This control requires that a documented security/vulnerability remediation action plan be created and maintained. This is a critical component, evaluated by government agencies, to assess the overall risk to processing, storing, or transmitting CUI by a nonfederal organization. To meet this control, customers should document their security/vulnerability remediation action plan consistent with the expectations of the control. OCI operations reviews the security posture of the control plane

The Core LZ defines a dynamic group for the Compute Agent to be used by the Compute management agent in the AppDev compartment which supports the deployment of OS Management.

Security Assessment: Security Control Monitoring CA.L2-3.12.3

This control emphasizes the ongoing assessment of security mechanisms deployed across the organization's infrastructure. The organization must implement processes to continuously monitor these controls, which involves tracking their performance, analyzing any incidents or anomalies, and verifying they are functioning as intended. Customer responsibilities include implementing software that tracks security control performance, conducting regular reviews and audits of security control data, addressing any vulnerabilities or incidents discovered during monitoring in a timely

manner and maintaining documentation of monitoring activities and actions taken to mitigate identified risks. OCI operations continuously monitors, tracks, and audits our security posture to manage the control plane, conduct administration, and deliver of customer support. Access is provided using a least privilege model. Customers can leverage OCI Cloud Guard to improve the overall security posture and have a holistic view of all the misconfigurations and monitor activities across tenancies and compartments with ease.

Security Assessment: System Security Plan CA.L2-3.12.4

The purpose of this control is to ensure that the organization has a clear and well-documented understanding of its systems, including their boundaries, environments, and security mechanisms. The System Security Plan (SSP) should provide a detailed description of identifying the limits of each system, including the hardware, software, and network components involved. The System Security Plan should describe the operational context in which the system functions, including the data it processes, users, and any relevant environmental conditions (e.g., physical, cloud, etc.). The customer is responsible for several key tasks related to this control by creating a detailed SSP that reflects the system's security posture, including documenting all security requirements and control implementations. The customer should periodically revise the SSP to account for changes in system architecture, new security controls, or any adjustments in the operational environment. The customer should ensure that all system connections are properly documented with corresponding security measures in place, working with internal stakeholders, such as IT, security, and management teams, to gather necessary information and ensure the plan accurately reflects the system. OCI keeps an updated SSP in conjunction with FedRAMP that customers may obtain through their Oracle sales representative.

System and Communications Protection: Boundary Protection SC.L2-3.13.1

This control secures the perimeter of the customer's solution, including the networks, ports, protocols used to interact with the customer's services, and data from both external and internal access. The customer may control internal access with OCI services and console-based tools, including the configuration of customer VCNs and gateways by the customer's administrator. The customer may configure firewalls for external protection and network security rules for added protection. The Core LZ implements secure, isolated networking which can address these controls. To isolate network traffic and provide boundary protection, subnets leverage route tables and security rules to provide simple protections for cloud resources.

Security Zones are associated with one or more compartments and a Security Zone recipe. When the customer creates and updates resources in a security zone, OCI validates these operations against the list of policies in the security zone recipe. If the action violates the customer's established policies, the operation is denied. Security Zones rely on Cloud Guard to detect policy violations. The combination of Cloud Guard and Security Zones provides powerful boundary protection for the customer's compartment. The customer may secure traffic between an on-premises network and a VCN, between the internet and a VCN, between subnets in a VCN using the intra-VCN routing capability to route traffic to the network firewall. OCI operations manages and monitors and secures the cloud boundary of the control plane, conducting administration, and delivery of customer support.

The Core LZ does not create OCI IAM users or API Keys of users. The Core LZ creates 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. The security list 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. The Core LZ deploys a Bastion network security group (NSG) for each VCN it creates. That NSG allows 22; however, the variable for ingress CIDRs does not allow 0.0.0.0/0. That NSG allows 3389; however, the variable for ingress CIDRs does not allow 0.0.0.0/0. The Core

LZ does not deploy any Oracle Integration Cloud instances. The Core LZ does not deploy any OAC instances. The Core LZ deploys VCNs with app subnets, which are private, that can be used for deploying OAC instances. The Core LZ does not deploy any ADB-S. The Core LZ deploys VCNs with database subnets, which are private, that can be used for deploying an ADB-S.

System and Communications Protection: Security Engineering SC.L2-3.13.2

This control emphasizes how organizations integrate systems security engineering principles into new systems and major upgrades, and, when feasible, into legacy system updates. This approach ensures secure, resilient systems by incorporating layered protections, security policies, threat modeling, and secure development practices. Applying these principles reduces risk and helps organizations manage disruptions and threats effectively. Customers can strengthen their security posture by incorporating security first design into their system and application architecture. Customers can leverage plethora of OCI services such as Cloud Guard, WAF, Firewall, etc. to tighten the security and monitor for incoming and outgoing traffic.

The Core LZ provisions the following compartments:

- Recommended enclosing compartment containing all compartments created
- Network compartment for all the networking resources, including the required network gateways
- Security compartment for the logging, key management, and notifications resources.
- App compartment for the application-related services, including Compute, Storage, Functions, Streams, Kubernetes nodes, API gateway, etc.
- Database compartment for all database resources
- Optional compartment for Oracle Exadata Database Service infrastructure

System and Communications Protection: Role Separation SC.L2-3.13.3

This control emphasizes the need to segregate roles within cloud environments to be assigned based on the user. Root level users such as administrators have higher-level access and responsibilities. By bifurcating the access for users to designated roles, organizations can reduce the likelihood of unauthorized system modification and improve the security by restricting access to sensitive system management functions. Customers can achieve this capability by defining roles and labeling users by the level of access, e.g., network administrator, storage administrator etc. and only assigning them to these components of the overall system. Implementing access control measures to enforce separation and restrict permissions for system management tasks to just admin accounts. Customers can leverage OCI IAM to create users, roles, and restrict access to only required users.

The Core LZ defines the following personas that account for most organizational needs:

- IAM Administrators: manage IAM services and resources including compartments, groups, dynamic groups, policies, identity providers, authentication policies, network sources, tag defaults. However, this group is not allowed to manage the out-of-box Administrators and Credential Administrators groups or modify the out-of-box Tenancy Admin policy.
- Credential Administrators: manage users capabilities and users credentials in general, including API keys, authentication tokens and secret keys.
- Cost Administrators: manage budgets and usage reports.
- Auditors: entitled with read-only access across the tenancy and the ability to use cloud-shell to run the cis_reports.py script.

- Announcement Readers: for reading announcements displayed in OCI Console.
- Security Administrators: manage security services and resources including Vaults, Keys, Logging, Vulnerability Scanning, Web Application Firewall, Bastion, Service Connector Hub.
- Network Administrators: manage OCI network family, including VCNs, Load Balancers, DRGs, VNICs, IP addresses.
- Application Administrators: manage application related resources including Compute images, OCI Functions, Kubernetes clusters, Streams, Object Storage, Block Storage, File Storage.
- Database Administrators: manage database services, including Oracle VMDB (Virtual Machine), BMDB (Bare Metal), ADB (Autonomous databases), Exadata databases, MySQL, NoSQL, etc.
- ExaCS Administrators (only created when ExaCS compartment is created): manage Exadata infrastructure and VM clusters in the ExaCS compartment.
- Storage Administrators: the only group allowed to delete storage resources, including buckets, volumes, and files. Used as a protection measure against inadvertent deletion of storage resources. OCI operations make sure any changes access happen via automated process and roles are exclusive to just the required service or feature.

The Core LZ modifies existing users. The Core LZ restricts OCI IAM policies for the Network Admins, Security Admins, App Admin, and Database Admins groups which allows them to create storage services but prevents them from deleting storage services. The Core LZ also creates a Storage Admin policy and group, which allows the deletion of storage resources but not their creation.

System and Communications Protection: Shared Resource Control SC.L2-3.13.4

This control is designed to mitigate the risk of leaking sensitive info inadvertently or accessed maliciously via shared system resources such as memory or disk. Customers can ensure that shared resources such as disk, memory, CPU resources are properly isolated to prevent leakage. Customers can leverage multiple services and features to avoid such inadvertent access to data such as Block volumes, File systems, Compute VCN. OCI has tightened monitoring and security in its control plane to make sure there is no such leakage. OCI Operations has layered security such as Bastion making, external traffic ingress into the cloud not possible.

System and Communications Protection: Public-Access System Separation SC.L2-3.13.5

This control involves separating internal systems from systems that users may access externally. The customer may use a demilitarized zone (DMZ) that puts the customer's public-facing services and websites on an isolated network that keeps systems that store data, such as the Oracle Database, on internal networks that are not directly accessible from the internet. Private subnets, Service Gateways, and NAT Gateways are standard tools to separate resources from public access that isolate services like databases from web servers, and provide access to cloud PaaS services without connecting to the public internet. A Dynamic Routing Gateway (DRG) acts as a virtual router, providing a path for traffic between the customer's on-premises networks and VCNs, and may be used to route traffic between VCNs. Custom network topologies may be constructed using components in different regions and tenancies with different types of attachments (e.g., VCN, RPC, etc.). Each DRG attachment has an associated route table which routes packets entering the DRG to their next hop. The customer may filter and separate internet traffic using Network Firewall, customer URL and Fully Qualified Domain Names (FQDN), and Intrusion detection and prevention. OCI Operations has layered security including the Bastion service which prohibits external traffic ingress into the cloud.

System and Communications Protection: Network Communication by Exception SC.L2-3.13.6

This control enforces a default-deny policy on network traffic, where all communication is blocked unless explicitly allowed based on pre-defined security rules. By implementing this strategy, organizations significantly minimize the attack surface and limit the potential for unauthorized traffic to move across their networks. Customers can use a combination of WAF and Network Firewall to implement deny policies. OCI uses intrusion detection and access monitoring tools to make sure traffic is denied by default and that only customer opened ports are available for traffic to ingress or egress.

The Core LZ creates an OCI event rule for Identity Provider changes, IDP mapping changes, IAM group changes, IAM policy changes, IAM User changes, VCN changes, network route table changes, network security group changes, and network gateway changes.

The Core LZ does not create OCI IAM users or API Keys of users. The Core LZ creates 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. 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. The Core LZ deploys a Bastion network security groups (NSG) for each VCN it creates. That NSG allows 22 however the variable for ingress CIDRs does not allow 0.0.0.0/0. That NSG allows 3389 however the variable for ingress CIDRs does not allow 0.0.0.0/0. The Core LZ does not deploy any Oracle Integration Cloud instances. The Core LZ does not deploy any OAC instances. The Core LZ deploys VCNs with app subnets, which are private, that can be used for deploying OAC instances. The Core LZ does not deploy any Autonomous Shared Databases (ADB-S). The Core LZ deploys VCNs with database subnets, which are private, that can be used for deploying an ADB-S.

The Core LZ does not deploy any Compute instance. The Core LZ deploys VCNs that can be used for deploying Compute instances, and the Secure Workload Module deploys Compute instances with the Legacy Metadata service endpoint disabled.

System and Communications Protection: Data in Transit SC.L2-3.13.8

This control highlights the importance of encryption for CUI data in transit so that if the data was to be intercepted, it cannot be modified or read. Customers can leverage OCI Site-to-Site VPN or use IPSec over FastConnect to encrypt the data. OCI has layered security with Yubikey, certificates, and continuous monitoring to prevent unauthorized access.

The Core LZ does not deploy any Compute instance. The Core LZ deploys VCNs that can be used for deploying Compute instances, and the Secure Workload Module deploys Compute instances with in-transit encryption enabled.

System and Communications Protection: Connections Termination SC.L2-3.13.9

This control is essential for securing systems by ensuring that communication sessions do not remain open unnecessarily, which could be exploited by unauthorized users or malicious actors. Customers are responsible for defining time limits for inactive sessions and implementing automated session timeouts to make sure the session ends. By ensuring re-authentication to reopen sessions after termination prevents unauthorized access. OCI Bastions, Load Balancer, databases, etc. have session termination features that customers can utilize to set timeouts. Internally, OCI uses session timers to terminate a session after a period of inactivity.

System and Communications Protection: Key Management SC.L2-3.13.10

This control requires organizations to establish and manage encryption keys for the cryptography used within the system. This can be manual or automated, and enacted in accordance with applicable laws, Executive Orders, policies, directives, regulations, and standards. To meet this

control, customers should design an encryption policy and manage keys as expected by the control. OCI encrypts data in transit and at rest in Oracle US Government Cloud with FIPS 140-2/3 validated encryption, and offers encryption products to enhance and simplify a customer's key management process. OCI operations has a mature key management system and policy for the management of the control plane, conducting administration, and delivery of customer support.

The Core LZ provisions the following compartments:

- Recommended enclosing compartment containing all compartments created.
- Network compartment for all the networking resources, including the required network gateways.
- Security compartment for the logging, key management, and notifications resources.
- App compartment for the application-related services, including Compute, Storage, Functions, Streams, Kubernetes nodes, API gateway, etc.
- Database compartment for all database resources.
- Optional compartment for Oracle Exadata Database Service infrastructure.

System and Communications Protection: CUI Encryption SC.L2-3.13.11

This control requires that all CUI data be protected using FIPS-validated cryptography. Information separation should also be used to limit access for those with the needed clearances, but not the necessary access approvals. To meet this control, customers should leverage the encryption of native cloud services and restrict exposing the data external devices (laptops, etc.), and use proper identity and access controls to limit access to only approved users. OCI encrypts data in transit and at rest in Oracle US Government Cloud with FIPS 140-2/3 validated encryption. OCI operations has no access to customer content with CUI for the management of the control plane, conducting administration, and delivery of customer support.

The Core LZ does not deploy any Compute instance. The Core LZ deploys VCNs that can be used for deploying Compute instances, and the Secure Workload Module deploys Compute instances with in-transit encryption enabled.

The Core LZ deploys an optional (Level 2 selected) OCI Vault in the Security Compartment and generates an optional CMK. It also deploys required OCI IAM policies for the Object Storage service and OCI IAM groups to use CMKs in the Security Compartment. The Core LZ deploys an optional Object Storage bucket in the AppDev Compartment. That bucket is deployed is deployed with versioning Enabled. It also deploys required OCI IAM policies for the Block Volume service and OCI IAM groups to use CMKs in the Security Compartment. It also deploys required OCI IAM policies for the Block Volume service and OCI IAM groups to use CMKs in the Security Compartment. It also deploys required OCI IAM policies for the FSS and OCI IAM groups to use keys in the Security Compartment.

System and Communications Protection: Data at Rest SC.L2-3.13.16

This control requires that all CUI data be stored and protected at rest through encryption, file share scanning or other data confidentiality tools. To meet this control, customers should leverage the encryption of native cloud services and restrict exposing the data external devices (laptops, etc.). OCI encrypts all data at-rest in OCI storage services. OCI operations has no access to customer content with CUI for the management of the control plane, conducting administration, and delivery of customer support.

The Core LZ deploys an optional (Level 2 selected) OCI Vault in the Security Compartment and generates an optional CMK. It also deploys required OCI IAM policies for the Object Storage service

and OCI IAM groups to use CMKs in the Security Compartment. The Core LZ deploys an optional Object Storage bucket in the AppDev Compartment. That bucket is deployed with versioning enabled. The Core LZ also deploys required OCI IAM policies for the Block Volume service and OCI IAM groups to use CMKs in the Security Compartment. The Core LZ deploys required OCI IAM policies for the Block Volume service and OCI IAM groups to use CMKs in the Security Compartment. The Core LZ deploys required OCI IAM policies for the FSS and OCI IAM groups to use keys in the Security Compartment.

System and Information Integrity: Flaw Remediation SI.L2-3.14.1

The flaw remediation control involves both the identification of a flaw and the correction of that flaw. These flaws can be firmware, software, corrective action patches, or software updates. There are multiple reporting sources for such flaws such as the Common Weakness Enumeration (CWE) and Common Vulnerabilities and Exposures (CVE) databases to assist in remediation. OCI offers native tools to show service level flaws including within the operating system (OS). Customers are responsible for monitoring the applications installed inside the customer's tenancy to ensure security vulnerabilities are addressed quickly. We recommend that the customer leverage existing tools to identify possible issues and have a documented incident response process that includes continuous monitoring, error handling, and security assessments.

Oracle Data Safe helps customers find potential security issues and provides recommendations on remediation. Oracle Data Safe Security Assessment helps the customer assess the security of their database configurations. It analyzes database configurations, user accounts, and security controls, and then reports the findings with recommendations for remediation activities that follow best practices to reduce or mitigate risk.

OCI operations monitors for announced flaws and reviews our own software/hardware and addresses flaws for the management of the control plane, conducting administration, and delivery of customer support.

The Core LZ defines a dynamic group for the Compute Agent to be used by the Compute management agent in the AppDev compartment which supports the deployment of OS Management.

System and Information Integrity: Malicious Code Protection SI.L2-3.14.2

This control is designed to protect against malicious code. This code can be in commercial or custom-built software and includes various cyberattacks that can compromise a service. This control seeks to implement prevention, detection, and safeguards. The malicious code protection control involves finding injection points for malicious code and providing a plan of defense. Malicious code can include viruses, worms, spyware, and Trojan horses. Frequent targets for malicious code that connect to the customer's solution can be firewalls, mail servers, web servers, proxy servers, and user hardware such as laptops, smart pads, and smart phones. Oracle offers solutions in our Marketplace to help review code that may fall under this control. In general, it is recommended to limit users from downloading data to external devices and to use identity tools to limit who has access to code for resources running in the customer's tenancy. OCI operations uses malicious code detection tools and processes for the management of the control plane, conducting administration, and delivery of customer support.

System and Information Integrity: Security Alerts & Advisories SI.L2-3.14.3

This control requires that the system is monitored for security alerts and advisories, and that appropriate action is taken. These alerts are made available from organizations such as the United States Computer Emergency Readiness Team (US-CERT) and various industry information sharing and analysis centers (ISACs). To meet this control, customers should monitor the sources listed

above and take the appropriate action. OCI operations monitors multiple sources to ensure we are notified of security alerts and appropriate action is taken for the management of the control plane, conducting administration, and delivery of customer support.

The Core LZ channels VCN flow logs and audit logs through Service Connector Hub (SCH) to Object Storage (by default), thus providing a consolidated view of logging data and making them more easily consumable by customers' SIEM and SOAR systems. The Core LZ channels VCN flow logs and audit logs through SCH to Object Storage (by default), thus providing a consolidated view of logging data and making them more easily consumable by customers' SIEM and SOAR systems.

System and Information Integrity: Update Malicious Code Protection SI.L2-3.14.4

This control is designed to protect against the constantly evolving risk from malicious code. This code can be in commercial or custom-built software, and includes various cyber-attacks that can compromise a service. This control seeks to update existing prevention, detection, and safeguards. To meet this control, customers should implement malicious code detection and protection procedures consistent with the expectations of the control

Malicious code attack controls are constantly evolving and adapting to industry defense measures, so it is important to monitor security alerts and advisories. ISVs and cloud service providers offer updates, and customers can use government provided services such as those from the Cybersecurity and Infrastructure Security Agency (CISA) to detect malicious code and take the appropriate action. OCI operations updates malicious code detection tools and processes for the management of the control plane, conducting administration, and delivery of customer support.

System and Information Integrity: Monitor Communications for Attacks SI.L2-3.14.6

This control requires internal and external monitoring of unusual/unauthorized use of the system network. Monitoring can be achieved through various intrusion detection, scanning, and monitoring techniques and tools including perimeter locations and all network connection. The output of these tools should be input into the incident respond and continuous monitoring programs. To meet this control, customers should implement intrusion detection and access monitoring procedures consistent with the expectations of the control. For OCI operations, Oracle uses intrusion detection and access monitoring tools for the management of the control plane, conducting administration, and delivery of customer support.

The Core LZ can be deployed to 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. The Core LZ channels VCN flow logs and Audit logs through SCH to Object Storage (by default), thus providing a consolidated view of logging data and making them more easily consumable by customers' SIEM and SOAR systems.

System and Information Integrity: Identify Unauthorized Use SI.L2-3.14.7

This control requires internal and external monitoring of unusual/unauthorized access or use of the system. Monitoring can be achieved through various intrusion detection, scanning, and monitoring techniques and tools. The output of these tools should be input into the incident response and continuous monitoring programs. To meet this control, customers should implement intrusion detection procedures consistent with the expectations of the control. OCI operations uses intrusion detection and access monitoring tools for the management of the control plane, conducting administration, and delivery of customer support.

The Core LZ channels VCN flow logs and audit logs through Service Connector Hub (SCH) to Object Storage (by default), thus providing a consolidated view of logging data and making them more easily consumable by customer SIEM and SOAR systems. The Core LZ can be configured to deploy

network security devices like third party Next Generation Firewalls from Checkpoint, Cisco, Fortinet, and Palo Alto Networks or the OCI Network Firewall. Learn more here about how the architecture funnels all traffic to these network security devices to leverage their security capabilities centrally.

Customer-Owned Responsibilities

CMMC Control	NIST SP 800-171 Control	OCI technology that assist meeting the control	Core LZ deploys OCI tools that can assist meeting the control
Access Control: Control CUI Flow AC.L2-3.1.3	3.1.3	IAM, Vault, Compartments, Identity, Bastions	IAM, Vault, Compartments
Access Control: Non-Privileged Account Use AC.L2-3.1.6	3.1.6	IAM	IAM
Access Control: Privileged Functions AC.L2-3.1.7	3.1.7	IAM, Audit	IAM
Access Control: Privacy & Security Notices AC.L2-3.1.9	3.1.9	IAM	N/A
Access Control: Wireless Account Authorization AC.L2-3.1.16	3.1.16	N/A	N/A
Access Control: Wireless Account Protection AC.L2-3.1.17	3.1.17	IAM, Identity	VCNs
Access Control: Mobile Device Connection AC.L2-3.1.18	3.1.18	N/A	N/A
Access Control: Encrypt CUI on Mobile AC.L2-3.1.19	3.1.19	IAM, Identity, Vault	IAM, Vault
Access Control: Portable Storage Use AC.L2-3.1.21	3.1.21	N/A	N/A
Access Control: Control Public Information AC.L2-3.1.22	3.1.22	IAM, Vault, Network Security Groups, Web Application Firewall, Security Lists	IAM, Vault, Block
Awareness and Training: Role-Based Risk Awareness AT.L2-3.2.1	3.2.1	N/A	N/A

CMMC Control	NIST SP 800-171 Control	OCI technology that assist meeting the control	Core LZ deploys OCI tools that can assist meeting the control
Awareness and Training: Role-Based Training AT.L2-3.2.2	3.2.2	N/A	N/A
Configuration Management: Security Impact Analysis CM.L2-3.4.4	3.4.4	N/A	N/A
Identification and Authentication: Password Complexity IA.L2-3.5.7	3.5.7	IAM, Identity	IAM
Identification and Authentication: Password Reuse IA.2-3.5.8	3.5.8	IAM, Identity	N/A
Identification and Authentication: Temporary Passwords IA.L2-3.5.9	3.5.9	IAM, Identity	N/A
Incident Response: Incident Response Testing IR.L2-3.6.3	3.6.3	N/A	N/A
System and Communications Protection: Split Tunneling SC.L2-3.13.7	3.13.7	N/A	N/A
System and Communications Protection: Collaborative Device Control SC.L2-3.13.12	3.13.12	N/A	N/A
System and Communications Protection: Mobile Code SC.L2-3.13.13	3.13.13	N/A	N/A

CMMC Control	NIST SP 800-171 Control	OCI technology that assist meeting the control	Core LZ deploys OCI tools that can assist meeting the control
System and Communications Protection: Voice over Internet Protocol SC.L2-3.13.14	3.13.14	N/A	N/A
System and Communications Protection: Communications Authenticity SC.L2-3.13.15	3.13.15	IAM, Virtual Cloud Networks, Network Security Groups, Security Lists	IAM, Vault, Object Storage, Network Security Groups, Security Lists
System and Information Integrity: System & File Scanning SI.L2-3.14.5	3.14.5	N/A	N/A

CMMC 2.0 Level 2 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.

Access Control: Control CUI Flow AC.L2-3.1.3

This control requires organizations to limit the flow of Controlled Unclassified Information (CUI) within their systems. This means ensuring that content with CUI is only transferred, shared, and accessed in ways that are in line with organizational policies and approved authorizations. The authorized access control includes different levels of access connections such as the OCI cloud administrator login, database permissions, web logins, and connections to external services. Access control in the customer's cloud environment can be simplified with a unified identity service such as Oracle Identity Domains where policies can be written to allow users access to resources within domains. The use of our Core LZ can simplify some aspects of access using Bastions and Vault as described in the Core LZ. Database tools can be configured to grant access or mask data for specific users.

The Core LZ defines the following personas that account for most organizational needs:

- IAM Administrators: manage IAM services and resources including compartments, groups, dynamic groups, policies, identity providers, authentication policies, network sources, tag defaults. However, this group is not allowed to manage the out-of-box Administrators and Credential Administrators groups or modify the out-of-box Tenancy Admin policy.

- Credential Administrators: manage users capabilities and users credentials in general, including API keys, authentication tokens and secret keys.
- Cost Administrators: manage budgets and usage reports.
- Auditors: entitled with read-only access across the tenancy and the ability to use cloud-shell to run the cis_reports.py script.
- Announcement Readers: for reading announcements displayed in OCI Console.
- Security Administrators: manage security services and resources including Vaults, Keys, Logging, Vulnerability Scanning, Web Application Firewall, Bastion, Service Connector Hub.
- Network Administrators: manage OCI network family, including VCNs, Load Balancers, DRGs, VNICs, IP addresses.
- Application Administrators: manage application related resources including Compute images, OCI Functions, Kubernetes clusters, Streams, Object Storage, Block Storage, File Storage.
- Database Administrators: manage database services, including Oracle VMDB (Virtual Machine), BMDB (Bare Metal), ADB (Autonomous databases), Exadata databases, MySQL, NoSQL, etc.
- ExaCS Administrators (only created when ExaCS compartment is created): manage Exadata infrastructure and VM clusters in the ExaCS compartment.
- Storage Administrators: the only group allowed to delete storage resources, including buckets, volumes, and files. Used as a protection measure against inadvertent deletion of storage resources.

The Core LZ deploys an optional (Level 2 selected) OCI Vault in the Security Compartment and generates an optional CMK. It also deploys required OCI IAM policies for the Object Storage service and OCI IAM groups to use CMKs in the Security Compartment. The Core LZ deploys an optional Object Storage bucket in the AppDev Compartment. That bucket is deployed is deployed with versioning enabled. It also deploys required OCI IAM policies for the Block Volume service and OCI IAM groups to use CMKs in the Security Compartment. It also deploys required OCI IAM policies for the FSS and OCI IAM groups to use keys in the Security Compartment.

Access Control: Non-Privileged Account Use AC.L2-3.1.6

This control highlights how customers must ensure that individuals with access to their systems use non-privileged accounts or roles when performing non-security-related tasks. This means assigning appropriate access levels based on the specific functions a user needs to perform. By limiting privileged account use to only critical security operations, customers reduce the risk of accidental or malicious misuse of system resources. Proper role-based access control not only enhances security but also helps maintain system integrity by ensuring users only have access to the resources and functions necessary for their responsibilities. Customers can leverage OCI IAM to assign roles to users to allow access to services that have predefined roles defined in Oracle Identity Cloud Service. Services managed through Identity Cloud Service can have two types of predefined roles—service access roles and instance access roles—which grant access to specific instances of a service.

The Core LZ defines the following personas that account for most organizational needs:

- IAM Administrators: manage IAM services and resources including compartments, groups, dynamic groups, policies, identity providers, authentication policies, network sources, tag

defaults. However, this group is not allowed to manage the out-of-box Administrators and Credential Administrators groups or modify the out-of-box Tenancy Admin policy.

- Credential Administrators: manage users capabilities and users credentials in general, including API keys, authentication tokens and secret keys.
- Cost Administrators: manage budgets and usage reports.
- Auditors: entitled with read-only access across the tenancy and the ability to use cloud-shell to run the cis_reports.py script.
- Announcement Readers: for reading announcements displayed in OCI Console.
- Security Administrators: manage security services and resources including Vaults, Keys, Logging, Vulnerability Scanning, Web Application Firewall, Bastion, Service Connector Hub.
- Network Administrators: manage OCI network family, including VCNs, Load Balancers, DRGs, VNICs, IP addresses.
- Application Administrators: manage application related resources including Compute images, OCI Functions, Kubernetes clusters, Streams, Object Storage, Block Storage, File Storage.
- Database Administrators: manage database services, including Oracle VMDB (Virtual Machine), BMDB (Bare Metal), ADB (Autonomous databases), Exadata databases, MySQL, NoSQL, etc.
- ExaCS Administrators (only created when ExaCS compartment is created): manage Exadata infrastructure and VM clusters in the ExaCS compartment.
- Storage Administrators: the only group allowed to delete storage resources, including buckets, volumes, and files. Used as a protection measure against inadvertent deletion of storage resources.

The Core LZ modifies existing users.

Access Control: Privileged Functions AC.L2-3.1.7

This control ensures that non-privileged users are prevented from executing privileged functions, and that the execution of privileged actions is captured in audit logs. Customers are accountable for establishing an effective auditing mechanism to track and record the execution of privileged functions within their systems. This involves setting up the necessary logging processes to monitor actions taken by users with elevated permissions. OCI Audit service, in conjunction with IAM, can be utilized to help implement this functionality, offering a structured way to maintain a record of privileged activities. By enabling such audits, customers gain visibility into who is performing sensitive operations, ensuring they can track and review access to critical system functions.

In addition to implementing auditing capabilities, customers are also responsible for properly configuring their systems to ensure that only authorized individuals are able to execute privileged functions. This includes setting appropriate user permissions and roles to prevent non-privileged users from accessing or performing tasks that require elevated permissions. Furthermore, it is critical that customers establish safeguards to protect their systems from being bypassed, altered, or disabled by unauthorized users. This involves ensuring that security controls are robust and cannot be easily circumvented, whether through technical means or process weaknesses.

By enforcing these configurations, customers not only protect their sensitive systems but also ensure compliance with security best practices. Unauthorized access to privileged functions poses significant risks, including the potential for data breaches, system misconfigurations, and other security incidents. Therefore, it is essential that customers take proactive steps to ensure that their

systems are appropriately secured and that any actions taken by privileged users are logged and auditable. Leveraging the Audit service and configuring user roles and security controls effectively will help customers maintain a secure and compliant environment while minimizing the risk of misuse or unauthorized access to critical functions.

The Core LZ defines the following personas that account for most organizational needs:

- IAM Administrators: manage IAM services and resources including compartments, groups, dynamic groups, policies, identity providers, authentication policies, network sources, tag defaults. However, this group is not allowed to manage the out-of-box Administrators and Credential Administrators groups or modify the out-of-box Tenancy Admin policy.
- Credential Administrators: manage users capabilities and users credentials in general, including API keys, authentication tokens and secret keys.
- Cost Administrators: manage budgets and usage reports.
- Auditors: entitled with read-only access across the tenancy and the ability to use cloud-shell to run the cis_reports.py script.
- Announcement Readers: for reading announcements displayed in OCI Console.
- Security Administrators: manage security services and resources including Vaults, Keys, Logging, Vulnerability Scanning, Web Application Firewall, Bastion, Service Connector Hub.
- Network Administrators: manage OCI network family, including VCNs, Load Balancers, DRGs, VNICs, IP addresses.
- Application Administrators: manage application related resources including Compute images, OCI Functions, Kubernetes clusters, Streams, Object Storage, Block Storage, File Storage.
- Database Administrators: manage database services, including Oracle VMDB (Virtual Machine), BMDB (Bare Metal), ADB (Autonomous databases), Exadata databases, MySQL, NoSQL, etc.
- ExaCS Administrators (only created when ExaCS compartment is created): manage Exadata infrastructure and VM clusters in the ExaCS compartment.
- Storage Administrators: the only group allowed to delete storage resources, including buckets, volumes, and files. Used as a protection measure against inadvertent deletion of storage resources.

The Core LZ modifies existing users.

Access Control: Privacy & Security Notices AC.L2-3.1.9

This control requires organizations to provide privacy and security notices that are consistent with the rules governing the handling of CUI. Customers are responsible for displaying a notification or banner to users before granting system access, which provides privacy and security notices in line with applicable federal laws, executive orders, and policies concerning U.S. government information. This notification must clearly communicate the relevant legal obligations and privacy guidelines. Additionally, customers must ensure that these banners remain visible on the screen until the user acknowledges the message. The acknowledgment optionally captured via a read receipt, should be retained for audit purposes to demonstrate compliance. Furthermore, customers must ensure that any publicly accessible information system presents users with a system usage notice before allowing further access. This information should outline the terms and conditions of system use, reinforcing security expectations and legal responsibilities.

Access Control: Wireless Access Authorization AC.L2-3.1.16

This control requires organizations to authorize wireless access before allowing connections to the organization's network. Customers are responsible for establishing and documenting usage restrictions, configuration and connection requirements, and implementation guidelines for wireless access in alignment with their access control policies. These guidelines must outline how wireless connections are managed and secured. Additionally, customers must ensure that wireless access to their systems is explicitly authorized before allowing any such connections. This proactive approach helps prevent unauthorized access and ensures that wireless usage complies with the organization's security standards and policies.

Access Control: Wireless Access Protection AC.L2-3.1.17

This control is focused on ensuring the security of wireless access by requiring users to authenticate before being granted access to an organization's wireless networks. Customers must establish and enforce authentication protocols for all users and devices attempting to connect to their wireless networks. Customers are responsible for properly configuring their wireless networks to require authentication before granting access. This includes setting up secure wireless protocols to prevent unauthorized access. Customers need to regularly monitor and audit wireless network connections to detect and respond to any unauthorized access attempts or anomalies.

The Core LZ does not deploy any Compute instance. The Core LZ deploys VCNs that can be used for deploying Compute instances, and the Secure Workload Module deploys Compute instances with in-transit encryption enabled.

Access Control: Mobile Device Connection AC.L2-3.1.18

This control highlights managing and controlling the connection of mobile devices (e.g., smartphones, tablets) to organizational systems and networks. Customers are responsible for defining and enforcing clear restrictions on how mobile devices can connect to their systems. Customers should ensure that all mobile devices are properly authenticated and authorized before granting access to sensitive systems.

Access Control: Encrypt CUI on Mobile AC.L2-3.1.19

This control focuses on protecting Controlled Unclassified Information (CUI) stored or accessed on mobile devices and mobile computing platforms by requiring encryption. Customers are responsible for ensuring that all CUI stored or accessed on mobile devices is encrypted. Customers need to choose encryption tools and technologies that are appropriate for the mobile devices and platforms in use within their organization. Customers must enforce encryption policies on all mobile devices used to access or store CUI. This includes ensuring that encryption is active and operational before allowing a device to access or store sensitive data.

The Core LZ deploys an optional (Level 2 selected) OCI Vault in the Security Compartment and generates an optional CMK. It also deploys required OCI IAM policies for the Object Storage service and OCI IAM groups to use CMKs in the Security Compartment. The Core LZ deploys an optional Object Storage bucket in the AppDev Compartment. That bucket is deployed with versioning enabled. The Core LZ deploys required OCI IAM policies for the Block Volume service and OCI IAM groups to use CMKs in the Security Compartment. The Core LZ also deploys required OCI IAM policies for the FSS and OCI IAM groups to use keys in the Security Compartment.

Access Control: Portable Storage Use AC.L2-3.1.21

This control is focused on limiting the use of portable storage devices (e.g., USB drives, external hard drives) on external systems. Customers are responsible for defining and enforcing policies that restrict the use of portable storage devices on external systems. These policies should limit or prevent the transfer of sensitive data to unauthorized or untrusted devices. Customers are

responsible for ensuring that portable storage devices are not used to store or transfer CUI to external systems that do not meet the organization's security requirements.

Access Control: Control Public Information AC.L2-3.1.22

This control focuses on ensuring that any information posted or processed on publicly accessible information systems is properly controlled. Customers are responsible for creating and enforcing policies and procedures that define what information can be posted or processed on publicly accessible systems. Before any data is posted to publicly accessible systems (such as websites or portals), customers must ensure it has been properly reviewed and approved. Customers must ensure that only non-sensitive information is posted on public platforms. CUI and other sensitive data should never be publicly accessible without appropriate safeguards.

The control of public information applies to the customer's cloud administrator access but is more focused on how and where the customer shares information. The customer controls which users have access to what data and how they interact with the data they share using an identity solution at the application or webpage level that includes terms of use. This requires a clear understanding of what information is sensitive and needs to be controlled through access limitations. Oracle Data Safe has a feature called Data Discovery which helps the customer find sensitive data in their databases. The customer specifies the data to search, and Data Discovery inspects the actual data in their database and its data dictionary. Data Discovery then returns to the customer a list of sensitive columns. By default, Data Discovery can search for a wide variety of sensitive data about personal identification, IT, financial, healthcare, employment, and academics.

The Core LZ deploys an optional (Level 2 selected) OCI Vault in the Security Compartment and generates an optional CMK. It also deploys required OCI IAM policies for the Object Storage service and OCI IAM groups to use CMKs in the Security Compartment. The Core LZ deploys an optional Object Storage bucket in the AppDev Compartment. That bucket is deployed with versioning enabled. The Core LZ deploys required OCI IAM policies for the Block Volume service and OCI IAM groups to use CMKs in the Security Compartment. The Core LZ deploys required OCI IAM policies for the FSS and OCI IAM groups to use keys in the Security Compartment.

Awareness and Training: Role-Based Risk Awareness AT.L2-3.2.1

This control emphasizes the importance of ensuring that key personnel, such as managers, system administrators, and users, are aware of the security risks associated with their roles and the policies, standards, and procedures relevant to maintaining the security of organizational systems. Customers must deliver tailored security awareness training that is relevant to the specific roles within the organization, such as managers, system administrators, and regular users. Customers are responsible for ensuring that employees are familiar with the organization's security policies, standards, and procedures. Security awareness is not a one-time effort; customers need to implement continuous training and reminders to ensure that all personnel remain up to date on emerging threats and security practices. Customers must ensure that personnel are aware of the unique security risks tied to their specific roles.

Awareness and Training: Role-Based Training AT.L2-3.2.2

This control focuses on ensuring that personnel receive appropriate training to perform their assigned information security duties and responsibilities effectively. Customers are responsible for creating and implementing security training programs that are specific to the roles and responsibilities of their personnel. Personnel assigned with security-related responsibilities must be properly trained on how to execute those duties. Customers should ensure that their role-based training programs are kept up to date with evolving security threats and new technologies. Customers must track the completion of security training for all personnel and verify that everyone has undergone the required role-specific training as personnel change roles or assume new

responsibilities. Customers are responsible for providing additional or updated training to ensure they are prepared for their new security duties.

Configuration Management: Security Impact Analysis CM.L2-3.4.4

This control focuses on evaluating the potential security effects of any changes to the organization's systems before those changes are implemented. Customers must perform a thorough security analysis of any proposed changes to their systems including software updates, hardware modifications, configuration changes, or new integrations. They should ensure that security impact assessments are a standard part of their change management process. Before any system modification is approved for deployment, it should undergo a security review to evaluate potential risks.

Identification and Authentication: Password Complexity IA.L2-3.5.7

This control requires organizations enforce minimum password complexity and ensure that users change certain characters when creating new passwords. Customers are responsible for developing and enforcing a password policy that defines the complexity requirements for user passwords. This policy should outline the minimum length, required types of characters (e.g., upper/lower case letters, numbers, symbols), and any prohibited practices such as using common or easily guessable passwords. When users create new passwords, customers must ensure that passwords differ significantly from previous ones. Customers need to configure their systems to enforce these complexity rules automatically. Most systems and applications allow for password policies to be enforced through settings that require users to meet specified complexity guidelines when creating or changing their passwords. Customers should periodically review and update password complexity requirements to ensure they remain effective against emerging password-cracking techniques, which may involve increasing the minimum password length or requiring more types of characters. While OCI IAM helps achieve this, customers should customize password to the desired complexity and train their employees on utilizing password complexity to enhance security posture.

The Core LZ defines four dynamic groups to satisfy common needs of workloads that are eventually deployed:

- Security Functions: to be used by functions defined in the Security compartment. The matching rule includes all functions in the Security compartment. An example is a function for rotating secrets kept in a Vault.
- AppDev Functions: to be used by functions defined in the AppDev compartment. The matching rule includes all functions in the AppDev compartment. An example is a function for processing of application data and writing it to an Object Storage bucket.
- Compute Agent: to be used by the Compute management agent in the AppDev compartment.
- Database KMS: to be used by databases in the Database compartment to access keys in the Vault service.

Identification and Authentication: Password Reuse IA.2-3.5.8

This control mandates that organizations prevent users from reusing the same password for a specified number of generations. Customers are responsible for setting up systems to track and enforce password reuse restrictions. Enforcing password reuse typically involves specifying how many previous passwords must be remembered by the system (e.g., the last 5, 10, or more passwords) to prevent them from being reused when a user changes their password. Customers must document a clear password reuse policy that specifies the number of generations for which old passwords cannot be reused. Customers need to configure their systems and applications to

automatically enforce the password reuse policy. Customers should regularly audit password change logs and monitor compliance with the password reuse policy. Customers should communicate the importance of password uniqueness to their users. Emphasizing that reusing passwords weakens security can help promote a stronger password culture and prevent users from seeking shortcuts when changing their credentials.

Identification and Authentication: Temporary Passwords IA.L2-3.5.9

This control requires organizations to allow the use of temporary passwords for system logons, with the condition that they must be changed immediately upon first use. Customers are responsible for issuing temporary passwords for system access, typically during user onboarding or password recovery. Customers must configure systems to require users to change their temporary passwords immediately upon their first logon, which ensures that the temporary credentials cannot be reused or exploited by unauthorized individuals. Customers should ensure that temporary passwords are short-lived, expiring if not used within a specific time frame.

Incident Response: Incident Response Testing IR.L2-3.6.3

This control requires organizations to regularly test their incident response capabilities. Before testing, customers are responsible for establishing a documented incident response plan that outlines roles, procedures, and communication strategies during an incident. Customers should schedule regular testing exercises, such as tabletop simulations, live drills, or red team/blue team exercises, to assess the readiness of their incident response team. Incident response tests should cover a range of possible scenarios, such as data breaches, denial of service attacks, or insider threats.

Systems and Communications Protection: Split Tunneling SC.L2-3.13.7

This control focuses on preventing remote devices from establishing simultaneous connections to both an organization's internal network and external, non-remote networks. Organizations are expected to ensure that their remote devices, such as laptops or mobile devices used by employees, do not engage in split tunneling while connected to the organization's network or systems. Ensuring that remote devices do not engage in split tunneling is crucial for preventing external or unsecured networks from acting as gateways for cyber threats. Customers must configure their devices and VPNs to block any attempt at split tunneling, meaning the device must only be connected to the internal network and should not have simultaneous access to external resources like public Wi-Fi or other internet services.

Customers are also responsible for ensuring that the organization's network configurations and security policies explicitly prohibit split tunneling for remote access. This may involve enforcing settings within the VPN infrastructure or endpoint protection solutions that prevent dual network connections. Additionally, customers need to continually monitor remote devices to ensure that split tunneling is not being re-enabled, either by mistake or maliciously, and must audit these settings regularly to maintain compliance with security standards and prevent potential data leaks or unauthorized access to their systems.

Systems and Communications Protection: Collaborative Device Control SC.L2-3.13.12

This control is focused on securing the use of collaborative computing devices such as video conferencing systems, smartboards, and other shared devices that allow remote collaboration. Customers are responsible for configuring their collaborative computing devices to prohibit remote activation unless explicitly authorized. It is the customer's responsibility to ensure that collaborative devices display clear and obvious indicators when they are in use.

Systems and Communications Protection: Mobile Code SC.L2-3.13.13

This control focuses on the management and oversight of mobile code within an organization's network and systems. Customers are responsible for implementing measures to control and monitor the use of such code to ensure that it does not compromise the security or integrity of their systems. To fulfill this responsibility, customers must establish policies and procedures for the safe use of mobile code. Customers should deploy security solutions that can monitor the execution of mobile code and detect any unusual or unauthorized behavior.

Systems and Communications Protection: Voice over Internet Protocol SC.L2-3.13.14

This control emphasizes the need for organizations to manage and oversee the implementation of Voice over Internet Protocol (VoIP) technologies within their networks. Customers should establish comprehensive policies governing the use of VoIP within their organization. Customers must ensure that proper encryption methods are employed to protect voice data during transmission, preventing interception by unauthorized parties.

Systems and Communications Protection: Communications Authenticity SC.L2-3.13.15

This control emphasizes communication sessions within an organization's network are authentic and have not been tampered with or intercepted. Customers are responsible for employing secure communication protocols that provide authentication and integrity checks also strong authentication mechanisms to verify the identities of the parties involved in communication sessions.

The Core LZ does not deploy any Compute instance. The Core LZ deploys VCNs that can be used for deploying Compute instances, and the Secure Workload Module deploys Compute instances with in-transit encryption enabled.

The Core LZ deploys an optional (Level 2 selected) OCI Vault in the Security Compartment and generates an optional CMK. It also deploys required OCI IAM policies for the Object Storage service and OCI IAM groups to use CMKs in the Security Compartment. The Core LZ deploys an optional Object Storage bucket in the AppDev Compartment. That bucket is deployed with versioning enabled. It also deploys required OCI IAM policies for the Block Volume service and OCI IAM groups to use CMKs in the Security Compartment. It also deploys required OCI IAM policies for the FSS and OCI IAM groups to use keys in the Security Compartment.

The Core LZ creates a security list for each VCN it creates. The security list 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. The Core LZ deploys a Bastion network security group (NSG) for each VCN it creates. That NSG allows port 22; however, the variable for ingress CIDRs does not allow 0.0.0.0/0. The Core LZ deploys a Bastion network security group (NSG) for each VCN it creates. That NSG allows 3389; however, the variable for ingress CIDRs does not allow 0.0.0.0/0. The Core LZ modifies the default security list for every VCN it creates to restrict all traffic except for ICMP. The Core LZ does not deploy any Oracle Integration Cloud instances. The Core LZ does not deploy any OAC instances. The Core LZ deploys VCNs with app subnets, which are private, that can be used for deploying OAC instances. The Core LZ does not deploy ADB-S. The Core LZ deploys VCNs with database subnets, which are private, that can be used for deploying an ADB-S.

System and Information Integrity: System & File Scanning SI.L2-3.14.5

This control requires all systems and files to be scanned for vulnerabilities, including operating systems and applications as well as any files stored on the customer's systems as part of their solution. Limiting external connections can minimize risk, but establishing a defined cadence to scan all systems containing files from external sources is necessary. OCI Vulnerability Scanning Service (VSS) helps improve the customer's security posture by routinely checking hosts and

container images for potential vulnerabilities. This service gives developers, operations, and security administrators comprehensive visibility into misconfigured or vulnerable resources and generates reports with metrics and details about these vulnerabilities including remediation information.

Customers are solely responsible for the system and file scanning control if their system includes multi-cloud or on-premises components.

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.

ORACLE

How to Complete CMMC Level 2 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
- Oracle Cloud Infrastructure Identity Domains
- CMMC website
- CMMC Self-Assessment Guide on the CMMC website
- CMMC Accreditation Body

ORACLE

Terms and Acronyms

3PAO	Third Party Assessment Organization
AC	Access Control
ADB	Autonomous Database
ADB-S	Autonomous Shared Database
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
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposure
CVSS	Common Vulnerabilities Scoring System
CWE	Common Weakness Enumeration
DbaaS	Database as a Service (BaseDB)
DIB	Defense Industrial Base
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
IA	Identification and Authentication
IaaS	Infrastructure as a Service
IAM	Oracle Cloud Infrastructure Identity and Access Management
IR	Incident Response
ISAC	Information Sharing and Analysis Center
IT	Information Technology
JAB	Joint Authorization Board (for FedRAMP)

LZ	Oracle Cloud Infrastructure Landing Zone
MA	Maintenance
MP	Media Protection
MSP	Managed Service Provider
NIST	National Institute of Standards and Technology
NSG	Network Security Group
NVD	National Vulnerability Database
OAC	Oracle Analytics Cloud
OCI	Oracle Cloud Infrastructure
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
SC	Systems and Communications
SCAP	Security Content Automated Protocol
SCH	Service Connector Hub
SI	System Information Integrity
SSP	System Security Plan
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	Oracle Cloud Infrastructure Vulnerability Scanning Service
WAF	Oracle Cloud Infrastructure Web Application Firewall

ORACLE

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