ORACLE

CMMC 2.0 Level 1 Guide

Guidance to achieve CMMC Level 1 compliance with OCI

November, 2024, Version [1.1]

Public

Purpose statement

This document is designed to provide guidance to the Defense Industrial Base community needing to achieve Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 1 compliance.

Disclaimer

This document and its attachment are 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 December 2023. 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

Introduction 4

Tools to help achieve CMMC 2.0 Level 1 4

Understanding the CMMC Level 1 controls 5

OCI Responsibilities 5

Shared Responsibilities 6

CMMC 2.0 Level 1 guidance for shared responsibilities 8

Access Control: 9

Transaction and Function Control AC.L1-b.1.ii 9

Access Control: External Connections AC.L1-b1.iii 10

Access Control: Control Public Information AC-L1-b.1.iv 10

Identification and Authentication: Identification IA-L1-b.1.v 11

Identification and Authentication: Authentication IA-L1-b.1.vi 11

System and Communications Protection: Boundary Protection SC-L1-b.1.x 12

System and Communications Protection: Public-Access System Separation SC-L1-b.1.xi 12

System and Information Integrity: Flaw Remediation SI-L1-b.1.xii 12

System and Information Integrity: Malicious Code Protection SI-L1-b.1.xiii 13

System and Information Integrity: Update Malicious Code Protection SI-L1-b.1.xiv 13

System and Information Integrity: System and File Scanning SI-L1-b.1.xv 13

How to Submit a CMMC Self-Assessment 15

Resources 15

Terms and Acronyms 16

Introduction

Defense Industrial Base (DIB) companies that store Federal Contract Information (FCI), and not Controlled Unclassified Information (CUI), must meet CMMC 2.0 Level 1 requirements. You need to review the data you store and manage as part of your US DoD 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 800-171/53 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.

You may inherit select OCI controls and simplify the achievement of CMMC Level 1 when running applications on OCI U.S. Government Cloud. It is important to understand that using a FedRAMP accredited cloud does not satisfy every control required by CMMC. This guide helps you understand which CMMC controls are your responsibility as well as which are shared with your managed service provide (MSP) and/or cloud service provider (CSP).

Achieving CMMC Level 1 compliance includes applying controls within your cloud environment, personnel, and data. Oracle may help you achieve these controls with our cloud native services and features as well as other enterprise solutions we offer that you may 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 chose 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 1 certification, and this guide can help you get started.

Tools to help achieve CMMC 2.0 Level 1

OCI offers three tools for helping you achieve your CMMC 2.0 Level 1 certification: this CMMC Level 1 guide, our Core Landing Zone (LZ) that has been assessed by the Center for Internet Security (CIS), and our CMMC Controls Checklist.

This OCI Core LZ Architecture Guide provides an overview of how organizations can use OCI to comply with the CMMC requirements. Landing Zones in OCI are pre-configured, secure, scalable environments that serve as a starting point for deploying workloads in the cloud using standard terraform. This guide is intended to help administrators understand OCI 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 CIS, to assist customers in meeting their portion of the CMMC control in the shared responsibility matrix. The OCI Core LZ is specifically designed to help organizations meet CMMC requirements efficiently. To access the LZ assets, administrators should navigate to the OCI LZs GitHub repository found here: https://github.com/oci-landing-zones/terraform-oci-core-landingzone.

Our CMMC Controls Checklist is an editable spreadsheet allowing you to track progress on CMMC compliance Level 1. Our checklist evaluates each control, shows OCI tools to meet your control obligations, details of the LZ assists with the control, allows you to add comments, and helps you manage your status for all 15 controls. You may use this checklist in combination with the documentation this guide describes to complete your CMMC self-assessment.

Understanding the CMMC Level 1 controls

OCI Responsibilities

CMMC Control	NIST SP 800-171 Control
Media Disposal MP.L1-b.1.vii	3.8.3
Limit Physical Access PE.L1-b.1.viii	3.10.1
Manage Visitors & Physical Access PE.L1-b.1.ix	3.10.3 (Escort Visitors)
Manage Visitors & Physical Access PE.L1-b.1.ix	3.10.4 (Physical Access Logs)
Manage Visitors & Physical Access PE.L1-b.1.ix	3.10.5 (Manage Physical Access)

While OCI owns the controls listed above, if you have a hybrid or on-premises cloud solution, you may need to evaluate more 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.

Media Protection: Media Disposal MP.L1-b.1.vii

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 uses rigid and auditable tools to manage these processes and ensures all media containing customer data is physically destroyed.

Physical Protection: Limit Physical Access PE.L1-b.1.viii

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: Manage Visitors & Physical Access PE.L1-b.1.ix

Escort Visitors

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 Access Logs

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

Manage Physical Access

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.

Shared Responsibilities

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.L1-b.1.i	3.1.1	Identity and Access Management (IAM)	IAM, Object Storage, Virtual Cloud Networks
Access Control: Transaction & Function Control AC.L1-b.1.ii	3.1.2	IAM	IAM, Object Storage
Access Control: External Connections AC.L1-b.1.iii	3.1.20	IAM, Virtual Cloud Networks: Subnets, Route Tables, and Security Rules	Virtual Cloud Networks, Security Lists
Access Control: Control Public Information AC.L1-b.1.iv	3.1.22	Organizational Policy	Organizational Policy
Identification and Authentication: Identification IA.L1-b.1.v	3.5.1	IAM, Identity	IAM
Identification and Authentication: Authentication IA-L1-b.1.vi	3.5.2	IAM, Identity	IAM
System and Communications Protection: Boundary Protection SC-L1-b.1.x	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: Public-Access System Separation SC-L1-b.1.xi	3.13.5	Virtual Cloud Networks, Cloud Guard, Security Zones, Subnets, Service Gateway, Dynamic Routing Gateway	NA
System and Information Integrity: Flaw Remediation SI-L1-b.1.xii	3.14.1	Cloud Guard, Audit	Dynamic Groups

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: Malicious Code Protection SI-L1-b.1.xiii	3.14.2	Web Application Firewall, Cloud Guard	NA
System and Information Integrity: Update Malicious Code SI-L1-b.1.xiv	3.14.4	Web Application Firewall, Cloud Guard	NA
System and Information Integrity: System & File Scanning SI-L1-b.1.xv	3.14.5	VSS	NA

ORACLE

CMMC 2.0 Level 1 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.L1-b.1.i

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 as described in the Core LZ. 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 and Function Control AC.L1-b.1.ii

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 the customer 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 which 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: External Connections AC.L1-b1.iii

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.

Our 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. Our Network Firewall service offers simple setup and deployment that gives the customer visibility into traffic entering the customer's 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. 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. 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 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. 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.

Access Control: Control Public Information AC-L1-b.1.iv

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 the customer's 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 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.

Identification and Authentication: Identification IA-L1-b.1.v

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-L1-b.1.vi

The authentication control requires verifying that the identity is who they claim to be. OCI administrators may control this through a password and multi-factor 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 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 multi-factor) to authenticate access the control plane, conducting administration, and delivery of customer support.

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

System and Communications Protection: Boundary Protection SC-L1-b.1.x

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 the customer's VCNs and gateways by their 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 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 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 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 a 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: Public-Access System Separation SC-L1-b.1.xi

This control involves separating internal systems from systems that users may access externally. The customer may use a demilitarized zone (DMZ) that puts their 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 Information Integrity: Flaw Remediation SI-L1-b.1.xii

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 their 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-L1-b.1.xiii

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: Update Malicious Code Protection SI-L1-b.1.xiv

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: System and File Scanning SI-L1-b.1.xv

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.

ORACLE

How to Submit a CMMC Self-Assessment

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

Resources

- OCI 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 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
AU	Audit and Accountability
BM	Bare Metal
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
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
FQDN	Fully Qualified Domain Names
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
USB	Universal Serial Bus
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 twitter.com/oracle