

# Secure Cloud Computing Architecture (SCCA) to NIST 800 Controls Mapping

Leveraging the Oracle Cloud Infrastructure SCCA Landing Zone to address NIST 800-171/53 control requirements

September, 2023, Version [\[1.0\]](#)

Copyright © 2023, Oracle and/or its affiliates

Public

## Purpose statement

This document highlights how you can use Oracle Cloud Secure Cloud Computing Architecture Landing Zone (SCCA LZ) to achieve NIST 800-171/53 controls. The Oracle Cloud SCCA LZ has been specifically designed and developed using Oracle Cloud Infrastructure (OCI) native services. This document will provide a high level overview of SCCA and NIST 800-53/171, and describe how United States (US) federal civilian and commercial customers can leverage the LZ to meet their regulatory requirements.

The SCCA LZ was designed for the US Department of Defense (DoD), however Oracle has made it available to all OCI customers. This document maps the SCCA requirements to applicable NIST SP 800-53/171 controls. These controls form the baseline for many compliance standards required by the US Government, including but not limited to FedRAMP, Impact Level (IL) 2/4, Criminal Justice Information Systems (CJIS), Internal Revenue Service (IRS) 1075, and StateRAMP controls. The Oracle US Government Cloud for IaaS/PaaS is FedRAMP High authorized which demonstrates that OCI has confirmed the implementation of 430 of the NIST 800-53 controls. However, within the cloud shared management model there are NIST controls that may be shared or owned by the customer. SCCA LZ is designed to assist customers in implementing and meeting their control requirements.

## 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. This document may reference products/services or security controls that currently are in the process of obtaining Defense Information Systems Agency (DISA) Impact Level 5 provisional authorization. Due to the nature of the document, it may not be possible to include all features described in this document. For additional information specific to certain Oracle Cloud Services with DISA Impact Level 5 authorization, please refer to this informational website, located at: [Oracle Cloud US Federal Cloud with DISA Impact Level 5 Authorization](#).*

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

*\* Oracle's CMMC 2.0 guidance is based on DoD Information (found at <https://dodcio.defense.gov/CMMC/>) and is current as of DEC 2021. Until the CMMC 2.0 changes become effective through both the title 32 CFR and title 48 CFR rulemaking processes, the U.S. Department of Defense will suspend the CMMC Piloting efforts and will not approve inclusion of a CMMC requirement in DoD solicitations. The CMMC 2.0 program requirements will not be mandatory until the title 32 CFR rulemaking is complete, and the CMMC program requirements have been implemented as needed into acquisition regulation through title 48 rulemaking.*

## Table of contents

---

<b>SCCA Overview</b>	<b>4</b>
<b>National Institute of Standards and Technology (NIST)</b>	<b>4</b>
<b>OCI SCCA Landing Zone (LZ) Architecture</b>	<b>5</b>
Compartments	5
Identity	5
Networking	6
Security	6
Monitoring	6
<b>Mapping SCCA controls to NIST</b>	<b>7</b>
<b>Conclusion</b>	<b>15</b>

## SCCA Overview

The purpose of Secure Cloud Computing Architecture (SCCA), as defined by Defense Information Systems Agency (DISA), is to provide a scalable, cost-effective approach to securing cloud-based programs under a common security architecture. This framework provides a consistent level of security that enables the use of commercially available Cloud Service Offerings (CSO) for hosting DoD mission applications operating at all DoD Information System Impact Levels (i.e., IL2, IL4, IL5).

The SCCA provides a standard approach for boundary and application-level security for DoD Impact Level 4 and 5 data hosted in multi-tenant commercial cloud environments.

### SCCA features the four components below:

- 1. Cloud Access Points (CAP):**  
The CAP provides access to the cloud, boundary protection of the Defense Information Systems Network (DISN) from the cloud, and cyber defense capabilities such as firewall and intrusion detection and prevention (IDS/IPS) at the DISN boundary.
- 2. Virtual Data Center Security Stack (VDSS):**  
The VDSS provides DoD Core Data Center (CDC)-like network security capabilities such as firewalls, intrusion detection, and intrusion prevention systems. It also provides application security capabilities such as Web Application Firewall (WAF) and proxy systems.
- 3. Virtual Data Center Managed Services (VDMS):**  
The VDMS provides system management network and mission owner system support services necessary to achieve Joint Information Environment (JIE) management plane connectivity and mission owner system compliance.
- 4. Trusted Cloud Credential Manager (TCCM):**  
The TCCM is an SCCA business role responsible for credential management with the purpose of enforcing least privilege access for privileged accounts that are established and managed using the cloud service provider's (CSP's) identity and access management system (IAM).

As either a commercial or federal civilian customer, you may use SCCA to enhance the security and reliability of your cloud computing environments. As a commercial customer, SCCA provides a robust framework that enables you to securely store and process sensitive data in the cloud as well as meet many of the shared and customer owned NIST controls. By implementing SCCA controls, you can continue to ensure your data, intellectual property, and other critical assets are protected against unauthorized access, data breaches, and other security threats.

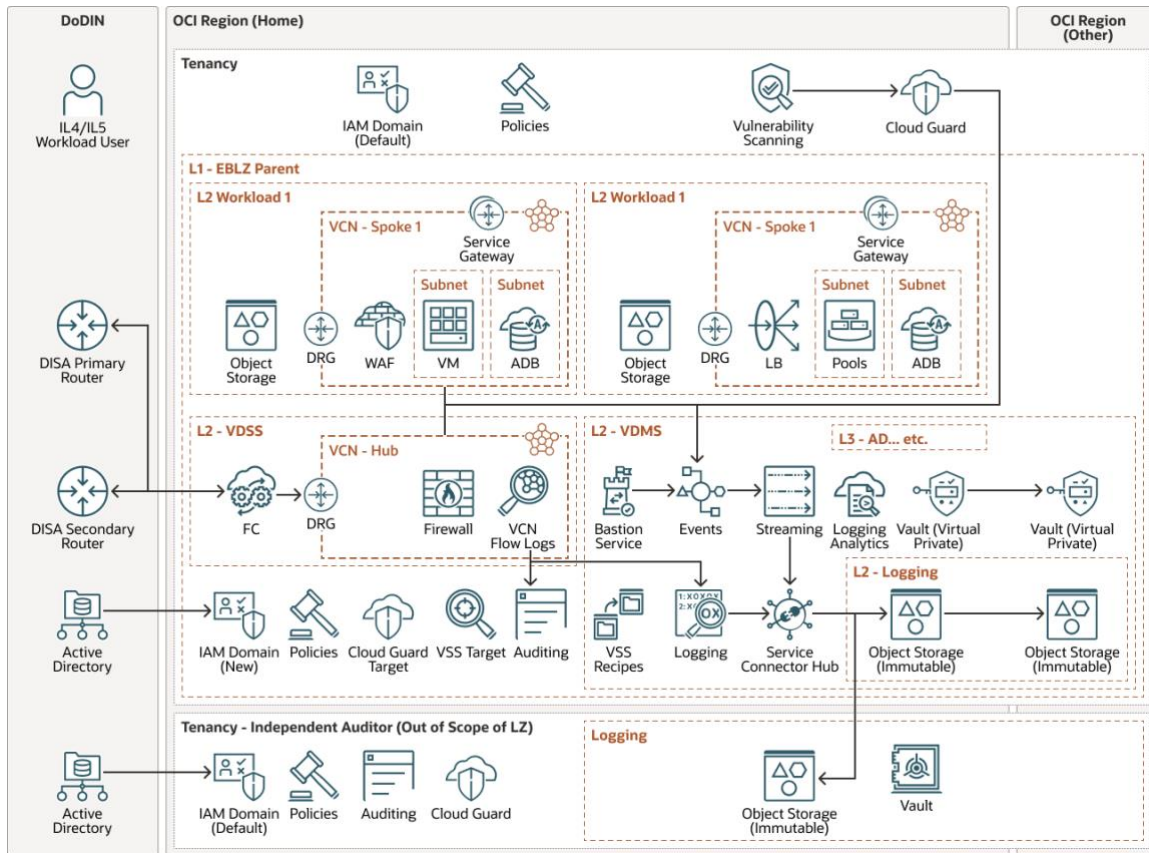
As a federal civilian customer, SCCA is particularly valuable as it aligns with the security requirements mandated by federal regulations, such as NIST 800-53/171. By implementing SCCA controls, federal agencies and organizations may ensure that their cloud environments meet the necessary security standards for protecting controlled unclassified information (CUI) and other sensitive data. SCCA provides a systematic approach to security that enables you to assess risks, implement appropriate controls, and monitor your cloud infrastructure effectively.

## National Institute of Standards and Technology (NIST)

NIST 800-171 controls are a set of requirements designed to protect controlled unclassified information (CUI) within non-federal systems and organizations. NIST 800-53 aims to protect federal information and information systems in non-federal organizations that collect or maintain information on behalf of a federal agency. These controls provide guidelines and security measures to safeguard sensitive information against unauthorized access, disclosure, alteration, and destruction. They cover various areas such as access control, incident response, configuration management, data protection, and system integrity. By implementing NIST controls, you can enhance your cybersecurity posture, meet compliance obligations, and ensure the confidentiality, integrity, and availability of CUI stored in your systems. These NIST controls form the baseline for almost all US government security compliance standards.

## OCI SCCA Landing Zone (LZ) Architecture

The below diagram represents the reference architecture for the Cloud Native SCCA LZ that provides the abstract building blocks for constructing a compliant SCCA .



## Compartments

The SCCA LZ creates a compartment structure that organizes the resources in a way that aligns with SCCA requirements. Below is the list of compartments that are deployed by the LZ.

- **Root Compartment:** This is deployed and available by default. It is not recommended to deploy any of your resources in this compartment.
- **SCCA Parent:** This is your parent compartment under which all other landing zone compartments will be created.
- **VDSS Compartment:** This contains your network and security components like network hub, firewall, and policies.
- **VDMS Compartment:** This contains all your managed services.
- **Backup Compartment:** This is used to store your configuration information in an object storage bucket.
- **Logging Compartment:** This is responsible for storing your log files in object storage.
- **Workload Compartment:** This contains your specific workload resources with a spoke connection to the main network hub.

SCCA architecture includes OCI components and services for Identity, Networking, Security, and Monitoring as detailed below.

## Identity

The SCCA LZ use Identity Domains to achieve identity and security. The X.509 feature flag will be enabled when the SCCA LZ is deployed. You will need to provide your own X.509 Identity Provider (IdP) which should also support the SAML Holder-of-Key profile. Once this is configured, federated users will be able to sign-in to the OCI Console with their Common Access Card (CAC) or Personal Identity Verification (PIV) Card. Identity is the keystone of security and can include providing access to everything from the OCI admin console to the database to web users accessing

information. In order to support SCCA access requirements with the above compartment configuration, the following Identity and Access Management (IAM) Groups will be deployed: VDSS Admin Group, VDMS Admin Group, and Workload Admin Group.

The following OCI cloud native services can be implemented with the SCCA LZ to help your organization meet SCCA security requirements.

- [IAM/Identity Domains](#)

## Networking

OCI enables the creation of virtual adaptations of conventional network elements. To protect north-south and east-west traffic flows, OCI recommends segmenting the network using a [hub and spoke topology](#), where traffic is routed through a central hub called Virtual Datacenter Security Stack (VDSS) virtual cloud network (VCN) and is connected to multiple distinct networks (spokes) called Virtual Datacenter Managed Services (VDMS) VCN and Workload VCNs.

All traffic between the VDMS and Workload compartments, whether to and from the internet, to and from an on-premises cloud environment, to the Oracle Services Network, or between them, is routed through the VDSS and inspected by Network Firewall multi-layered threat prevention technology. Each tier of Workload will be deployed in a VCN, which acts as a spoke. The VDSS VCN contains a Network Firewall based on Palo Alto Technologies, an Oracle internet gateway, a Dynamic Routing Gateway, and an Oracle Service Gateway.

The following OCI cloud native services can be implemented with the SCCA LZ to help your organization meet SCCA security requirements.

- [Network Firewall](#)
- [WAF](#)
- [VTAP](#)

## Security

OCI is a security-first cloud infrastructure that helps organizations reduce the risk of security threats for cloud workloads by putting your data security and privacy first. This is achieved via the automation of security operations with simple, prescriptive, and integrated cloud native security capabilities built into the OCI platform. Oracle provides the services and features to help you easily adopt OCI services and secure your cloud environment, applications, and data.

The following OCI cloud-native services can be implemented with the SCCA LZ to help your organization meet SCCA security requirements and use VDMS to meet NIST requirements.

- [Vault \(Key Management\)](#)
- [Log Archiving Storage Bucket](#)
- [Streaming](#)
- [Events](#)
- [Default Log Group](#)
- [Service Connector](#)
- [Vulnerability Scanning Service \(VSS\)](#)
- [Cloud Guard](#)

## Monitoring

The SCCA LZ provides several services that work together to provide monitoring capabilities across your tenancy. This creates a structure in the VDSS, VDMS, and Workload components to capture monitoring and log data that can be used to demonstrate implementation and continuous monitoring of your cloud environment. To minimize monitoring costs and irrelevant messaging, the landing zone deployment will have these alerts disabled by default. Based upon your operational model, you can enable the relevant alerts from the Oracle Cloud console.

The following OCI cloud native services can be implemented with the SCCA LZ to help your organization meet SCCA security requirements.

- [Logging Analytics](#)
- [Audit](#)
- [Logs](#)
- [Observability and Management](#)

## Mapping SCCA controls to NIST

NIST 800-171/53 control requirements are applicable across public and private sector frameworks, including CJIS, FedRAMP, and Cloud Computing Security Requirements Guide (CC SRG). The table below maps the SCCA requirements that can be implemented with the SCCA LZ to NIST 800-171/53 control requirements. This mapping will help you evaluate the applicability of the SCCA LZ as it relates to other frameworks that rely on these NIST controls.

The mapping in the table below is for informational purposes only and you are responsible for determining how SCCA and NIST requirements should be implemented in your environment.

### NIST800-171/53 to SCCA Mappings

SCCA Req-ID	SCCA Description	NIST 800 control		NIST Description	OCI Service
		171R2	53R4		
2.2.4.3	The Internal Cloud Access Point (ICAP) shall allow the transfer of security sensor data from the mission owner virtual networks to the Defense Information Systems Network (DISN) management	3.1.3	SC-7, SA-8	Control the flow of CUI in accordance with approved authorizations.	OCI Networking
2.2.4.4	The ICAP shall provide network traffic isolation between the CSP's privileged user (i.e., CSP Personnel) management network and DoD Mission Owner virtual networks.	3.1.15	AC-17(4)	Authorize remote execution of privileged commands and remote access to security-relevant information.	Identity Domains, IAM, OCI Networking
2.1.2.1	The Virtual Datacenter Security Stack (VDSS) shall maintain virtual separation of all management, user, and data traffic.	3.1.4, 3.13.3,	AC-5, SC-2,	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	IP Address Manager (IPAM) Security List VCN Subnets, Identity Domain



<p><b>2.1.2.10</b></p>	<p>The VDSS shall provide an interface to conduct ports, protocols, and service management (PPSM) activities in order to provide control for operators.</p>	<p>3.12.1,3.4.2</p>	<p>CA-2, CA-5, CA-7, CM-2, CM-6, CM-8, CM-8(1)</p>	<p>Establish and enforce security configuration settings for information technology products employed in organizational systems.</p>	<p>OCI Security List Network Firewall</p>
<p><b>2.1.2.11</b></p>	<p>The VDSS shall provide a monitoring capability that captures log files and event data for cybersecurity analysis.</p>	<p>3.13.1, 3.3.1</p>	<p>SC-7, SA-8, AU-2, AU-3, AU-3(1), AU-6, AU-12</p>	<p>Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.</p>	<p>Logging Analytics OCI Logging OCI Monitoring</p>
<p><b>2.1.2.12</b></p>	<p>The VDSS shall provide or feed security information and event data to an allocated archiving system for common collection, storage, and access to event logs by privileged users performing Boundary and Mission Computer Network Defense (CND) activities</p>	<p>3.1.7</p>	<p>AC-6(9), AC-6(10)</p>	<p>Privileged functions include establishing system accounts, performing system integrity checks, conducting patching operations, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users. Note that this requirement represents a condition to be achieved by the definition of authorized privileges in 3.1.2. Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse</p>	<p>Logging, Service Connector Hub, Object Storage</p>



				impacts on organizations. Logging the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat.	
<b>2.1.2.13</b>	The VDSS shall provide a FIPS-140-2 compliant encryption key management system for storage of DoD generated and assigned server private encryption key credentials for access and use by the Web Application Firewall (WAF) in the execution of SSL/TLS break and inspection of encrypted communication sessions.	3.13.10 03.13.11 3.1.13	SC-12, SC-13 AC-17(2)	Cryptographic key management and establishment can be performed using manual procedures or mechanisms supported by manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, policies, directives, regulations, and standards specifying appropriate options, levels, and parameters. DISA Special Publication [SP 800-56A] and [SP 800-57-1] provide guidance on cryptographic key management and key establishment.	Virtual Private Vault
<b>2.1.2.14</b>	The VDSS shall provide the capability to detect and identify application session hijacking	3.13.15	SC-23	Protect the authenticity of communications sessions.	Network Firewall OCI WAF
<b>2.1.2.15</b>	The VDSS shall provide a DoD demilitarized zones (DMZ) Extension to support Internet Facing Applications (IFAs)	3.13.5	SC-7	Subnetworks that are physically or logically separated from internal networks are referred to as DMZs. DMZs are typically implemented with boundary control devices and techniques that include routers, gateways, firewalls, virtualization, or cloud-based technologies. [SP 800-41] provides guidance on firewalls and firewall policy. [SP 800-125B] provides guidance on security for virtualization technologies.	Network Firewall OCI WAF

2.1.2.16	The VDSS shall provide full packet capture (FPC) or cloud service equivalent FPC capability for recording and interpreting traversing communication.	3.3.1, 3.1.3	AU-2, AU-3, AU-3(1), AU-6, AU-12	Control the flow of CUI in accordance with approved authorizations.	VTAP
2.1.2.17	The VDSS shall provide network packet flow metrics and statistics for all traversing communication.	3.3.1, 3.1.3	AU-2, AU-3, AU-3(1), AU-6, AU-12	Control the flow of CUI in accordance with approved authorizations.	VTAP
2.2.1.18	The VDSS shall provide for the inspection of traffic entering and exiting each mission owner virtual private network.	3.3.1, 3.1.3	AU-2, AU-3, AU-3(1), AU-6, AU-12, AU-11	Control the flow of CUI in accordance with approved authorizations.	VTAP
2.1.2.2	The VDSS shall allow the use of encryption for segmentation of management traffic.	3.13.5,3.13.6	SC-7(5)	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	VCN
2.1.2.4	The VDSS shall provide a capability to inspect and filter application layer conversations based on a predefined set of rules (including HTTP) to identify and block malicious content.	3.1.3	AC-4	Control the flow of CUI in accordance with approved authorizations.	Network Firewall OC WAF
2.1.2.5	The VDSS shall provide a capability that can distinguish and block unauthorized application layer traffic.	3.13.6	SC-7(5)	Employ the principle of least privilege, including for specific security functions and privileged accounts.	OCI WAF Network Firewall OCI Observability and Management Platform
2.1.2.6	The VDSS shall provide a capability that monitors network and system activities to detect and report malicious activities for traffic entering and exiting Mission Owner virtual private networks/enclaves.	3.13.1	SC-7	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	OCI WAF Network Firewall OCI Observability and Management Platform
2.1.2.7	The VDSS shall provide a capability that monitors network and system activities to stop or block detected malicious activity.	3.1.12, 3.13.1	SC-7 AC-17(1)	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries	WAF/Network Firewall, Oracle Cloud Observability, and

				and key internal boundaries of organizational systems.	Management Platform
<b>2.1.2.8</b>	The VDSS shall inspect and filter traffic traversing between mission owner virtual private networks/enclaves.	3.1.12, 3.13.1	SC-7 AC-17(1)	This requirement addresses security-related issues with maintenance tools that are not within the organizational system boundaries that process, store, or transmit CUI, but are used specifically for diagnostic and repair actions on those systems.	WAF/Network Firewall, Oracle Cloud Observability and Management Platform
<b>2.1.2.9</b>	The VDSS shall perform break and inspection of secure sockets layer and transport layer security (SSL/TLS) communication traffic supporting single and dual authentication for traffic destined to systems hosted within the Cloud Service Environment (CSE).	3.13.1	SC-7	This requirement addresses security-related issues with maintenance tools that are not within the organizational system boundaries that process, store, or transmit CUI, but are used specifically for diagnostic and repair actions on those systems.	WAF/Network Firewall, Oracle Cloud Observability and Management Platform
<b>2.3.1.2</b>	The VDSS shall provide cloud service offering (CSO) resident or remotely hosted mission enclave perimeter protection and sensing.	3.14.6	SI-4, SI-4 (4)	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Network Firewall
<b>2.3.2.2</b>	SCCA component managers shall be able to manage (e.g., set security, configuration, & routing policies and install patches) SCCA system security and network components.	3.1.3	AC-4	Control the flow of CUI in accordance with approved authorizations.	APIs OCI Console Security List OS Management
<b>2.3.2.3</b>	SCCA component managers shall allow for the configuration, control, and management of Ports, Protocols, and Services Management (PPSM) in accordance with DoDI 8551.01.	3.14.6 3.13.1	SI-4, SI-4(4) SC-7	Establish and enforce security configuration settings for information technology products employed in organizational systems.	OCI Networking Network Firewall
<b>2.3.2.6</b>	SCCA components shall provide logically separate network interfaces for access from the management network infrastructure that is logically separate from production.	3.13.5	SC-7, SA-8	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	OCI Networking

2.3.2.9	SCCA components shall provide management traffic segmentation from user and data plane traffic.	3.1.3	AC-4	Control the flow of CUI in accordance with approved authorizations.	OCI Networking
2.4.2.1	The VDSS unit processing latency shall be no greater than 35 milliseconds.	3.1.3	AC-4	Control the flow of CUI in accordance with approved authorizations.	Oracle Cloud Networking
2.4.2.5	The VDSS shall support IP packet forwarding in accordance with Mission Owner Differentiated Services Code Point (DSCP) tagged Quality of service (QOS) prioritization.	3.1.3	AC-4	Control the flow of CUI in accordance with approved authorizations.	Oracle Cloud Networking
2.5.2.1	The VDSS management systems shall provide a mechanism for managing failover in accordance with DoD Unified Capabilities Requirements (UCR) 2013.	3.1.3	AC-4	Control the flow of CUI in accordance with approved authorizations.	Oracle Cloud Networking
2.5.2.2	The VDSS management systems shall provide the capability to ensure all SCCA element configurations and policies are recoverable.	3.1.3	AC-4	Control the flow of CUI in accordance with approved authorizations.	Oracle Cloud High Availability Networking
2.5.2.3	The VDSS shall maintain offsite backup configurations for the recovery of operation.	3.8.9	CP-9	Protect the confidentiality of backup CUI at storage locations.	Cross-region Replication (Object Storage)
2.7.2.1	The VDSS shall provide the ability to backup and restore security, network, account, and system configurations.	3.8.9,	CP-9,	Protect the confidentiality of backup CUI at storage locations.	Backup, Object storage, Archive storage
2.7.2.2	The VDSS shall provide the capability to backup configuration and system data of all VDSS elements.	3.8.9	CP-9	Protect the confidentiality of backup CUI at storage locations.	Backup, Object storage, Archive storage
2.7.2.3	The VDSS shall provide the means to restore operational capability.	3.8.9	CP-9	Protect the confidentiality of backup CUI at storage locations.	Backup, Object storage, Archive storage
2.1.3.2	The VDMS shall provide Host Based Security System (HBSS), or approved equivalent, to manage endpoint security for all enclaves within the CSE.	3.11.2	RA-5, RA-5(5)	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	VSS

<p><b>2.1.3.4</b></p>	<p>The VDMS shall provide a configuration and update management system to serve systems and applications for all enclaves within the CSE.</p>	<p>3.4.1</p>	<p>CM-2, CM-6, CM-8</p>	<p>Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.</p>	<p>Oracle Cloud Resource Manager, OS Management Service, YUM</p>
<p><b>2.1.3.6</b></p>	<p>The VDMS shall provide a network for managing systems and applications within the CSE that is logically separate from the user and data networks.</p>	<p>3.13.5</p>	<p>SC-7</p>	<p>Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.</p>	<p>DRG, VCN Attachment, Security List, VCN, Subnets</p>
<p><b>2.1.3.7</b></p>	<p>The VDMS shall provide a system, security, application, and user activity event logging and archiving system for common collection, storage, and access to event logs by privileged users performing Boundary Cyberspace Protection (BCP) and Mission Cyberspace Protection (MCP) activities.</p>	<p>3.1.7,3.3.1</p>	<p>AC-6(9), AC-6(10), AU-2, AU-3,AU-3(1)</p>	<p>Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.</p>	<p>Object Storage, Archive Storage, OCI Logging</p>
<p><b>2.1.3.8</b></p>	<p>The VDMS shall provide for the exchange of DoD privileged user authentication and authorization attributes with the CSP's Identity and access management system to enable cloud system provisioning, deployment, and configuration.</p>	<p>3.5.1, 3.5.2</p>	<p>IA-2, IA-5</p>	<p>Identify system users, processes acting on behalf of users, and devices.  Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.</p>	<p>Oracle Identity Cloud Services (IDCS) IAM</p>
<p><b>2.2.3.3</b></p>	<p>The VDMS shall provide secure connectivity to mission owner management systems inside the CSO that is logically separate from mission application traffic.</p>	<p>3.13.1, 3.13.15</p>	<p>SC-7, SA-8 SC-23</p>	<p>Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.</p>	<p>Networking</p>
<p><b>2.3.2.4</b></p>	<p>SCCA component managers shall provide a capability to implement and control system configuration, report configuration change</p>	<p>3.3.2, 3.4.1</p>	<p>AU-2, AU-3, AU-3(1), AU-6, AU-12,</p>	<p>Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.</p>	<p>OCI Resource Manager</p>

	incidents, and support DoD component change configuration management systems and processes.		CM-2, CM-6, CM-8, CM-8(1)		
<b>2.3.3.2</b>	SCCA security elements shall provide performance data, such as CPU, bandwidth, memory and disk I/O, and storage utilization to SCCA management systems for performance analysis and reporting.	3.1.7, 3.3.1 3.13.1	AC-6(9), AC-6(10), AU-2, AU-3, AU-3(1), AU-6, AU-12,SC-7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	OCI Monitoring, Metrics, Logging
<b>2.3.3.3</b>	The SCCA security elements shall be able to generate reports and alerts based on performance information provided by SCCA systems.	3.1.7, 3.3.1 3.13.1	AC-6(9), AC-6(10), AU-2, AU-3, AU-3(1), AU-6, AU-12,SC-7	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	OCI Monitoring Metrics Logging
<b>2.3.5.1</b>	The FPC shall support integration with log insight detector systems to effect data search and retrieval, such as the capability to pull select timeframes of captured data.	3.3.1, 3.1.3	AU-2, AU-3, AU-3(1), AU-6, AU-12	Control the flow of CUI in accordance with approved authorizations.	VTAP (Customers are responsible for Log Insight Detector)
<b>2.3.5.4</b>	The FPC shall provide a capability to request an arbitrary subset of packets.	3.3.1, 3.1.3	AU-2, AU-3, AU-3(1), AU-6, AU-12, AC-4	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	OCI VTAP
<b>2.3.5.5</b>	The FPC shall locally store captured traffic for 30 days.	3.3.1, 3.1.3	AU-2, AU-3, AU-3(1), AU-6, AU-12, AC-4	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	OCI VTAP
<b>2.3.5.6</b>	The FPC data shall be isolated from user and data plane traffic via cryptographic or physical means.	3.3.1, 3.1.3	AU-2, AU-3, AU-3(1), AU-6, AU-12, AC-4	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	OCI VTAP
<b>2.3.5.8</b>	The FPC function shall be configurable according to	3.3.1, 3.1.3	AU-2, AU-3, AU-3(1),	Create and retain system audit logs and records to	OCI VTAP

	traffic flow source and destination points to avoid multiple point capture.		AU-6, AU-12	the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	
--	---	--	-------------	---	--

## Conclusion


The SCCA LZ configures multiple OCI native services that have achieved FedRAMP High and DISA IL2/4 authorization in Oracle Government Cloud. Please note, the OCI SCCA LZ is available at no cost, however the usage of OCI services that the SCCA LZ configures may have a cost associated with consumption of the service. Please evaluate this cost as part of your overall security posture program.


## Resources


- [SCCA LZ available here on GitHub](#)
- [Oracle Cloud Native SCCA Landing Zone – Architecture Guide](#)
- [Oracle Cloud Native SCCA Landing Zone – Customer Responsibility Guide](#)
- [Deploy SCCA-compliant workloads using Oracle Cloud Native SCCA Landing Zone](#)

### 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](https://blogs.oracle.com)

 [facebook.com/oracle](https://facebook.com/oracle)

 [twitter.com/oracle](https://twitter.com/oracle)

Copyright © 2023, Oracle and/or its affiliates. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.