ORACLE

Advisory: Oracle Cloud Infrastructure and the North American Electric Reliability Corporation Critical Infrastructure Protection Standards

Description of Oracle Cloud Infrastructure Security Practices in the Context of the NERC CIP Standards

December 2022, Version 1.0

Public

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. This document is not part of your agreement, nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you assessing your use of Oracle Cloud Infrastructure (OCI) in the context of the requirements applicable to you under the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards. This document might also help you to assess Oracle as an outsourced service provider. You remain responsible for making your own independent assessment of the information in this document, which is not intended and may not be used as legal advice about the content, interpretation, or application of laws, regulations, and regulatory guidelines. You should seek independent legal advice regarding the applicability and requirements of laws and regulations discussed in this document.

This document does not make any commitment to deliver any material, code, or functionality, and should not be relied on in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

The NERC CIP Standards are subject to periodic changes or revisions by NERC. The current version of the NERC CIP Standards is available at www.nerc.com/pa/Stand/AlignRep/Mandatory%20Standards%20Subject%20to%20Enforcement.xlsx. This document is based on information available at the time of drafting. It is subject to change at the sole discretion of Oracle Corporation and might not always reflect changes in the regulations.

Table of Contents

Introduction

The North American Electric Reliability Corporation (NERC) is a not-for-profit regulatory authority whose aim is to ensure "effective and efficient reduction of risks to the reliability and security of the bulk power grid." NERC develops and enforces reliability standards and is subject to oversight by the US Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. The NERC Critical Infrastructure Protection (CIP) cybersecurity standards establish a range of security programs for the power industry within the US and Canada. For more information, see www.nerc.com/AboutNERC/Pages/default.aspx.

Document Purpose

This document is intended to provide relevant information related to Oracle Cloud Infrastructure (OCI) to assist you in determining the suitability of using OCI services for non-mission-critical workloads in relation to the NERC CIP standards.

The information contained in this document does not constitute legal advice. Customers are advised to seek their own legal counsel to develop and implement their compliance program and to assess the features and functionality provided by Oracle in regard to their specific legal and regulatory requirements.

About Oracle Cloud Infrastructure

Oracle's mission is to help customers see data in new ways, discover insights, and unlock possibilities. Oracle provides several cloud solutions tailored to customers' needs. These solutions provide the benefits of the cloud, including global, secure, and high-performance environments in which to run all your workloads. The cloud offerings discussed in this document include OCI.

OCI is a set of complementary cloud services that enable you to build and run a wide range of applications and services in a highly available and secure hosted environment. OCI offers high-performance computing capabilities and storage capacity in a flexible overlay virtual network that is easily accessible from an on-premises network. OCI also delivers high-performance computing power to run cloud native and enterprise IT workloads. For more information about OCI, see docs.oracle.com/en-us/iaas/Content/home.htm.

The Cloud Shared Management Model

From a security management perspective, cloud computing is fundamentally different from on-premises computing. On-premises customers are in full control of their technology infrastructure. For example, they have physical control of the hardware and full control over the technology stack in production. In the cloud, however, customers use components that are partially under the management of the cloud service providers. As a result, the management of security in the cloud is a shared responsibility between the cloud customers and the cloud service provider.

Oracle provides best-in-class security technology and operational processes to secure enterprise cloud services. However, customers must also be aware of and manage their security and compliance responsibilities when running their workloads in Oracle cloud services. By design, Oracle provides security functions for cloud infrastructure and operations, such as cloud operator access controls and infrastructure security patching. Customers are responsible for securely configuring and using their cloud resources. For more information, see the cloud service documentation.

The following figure illustrates this division of responsibility at high level.

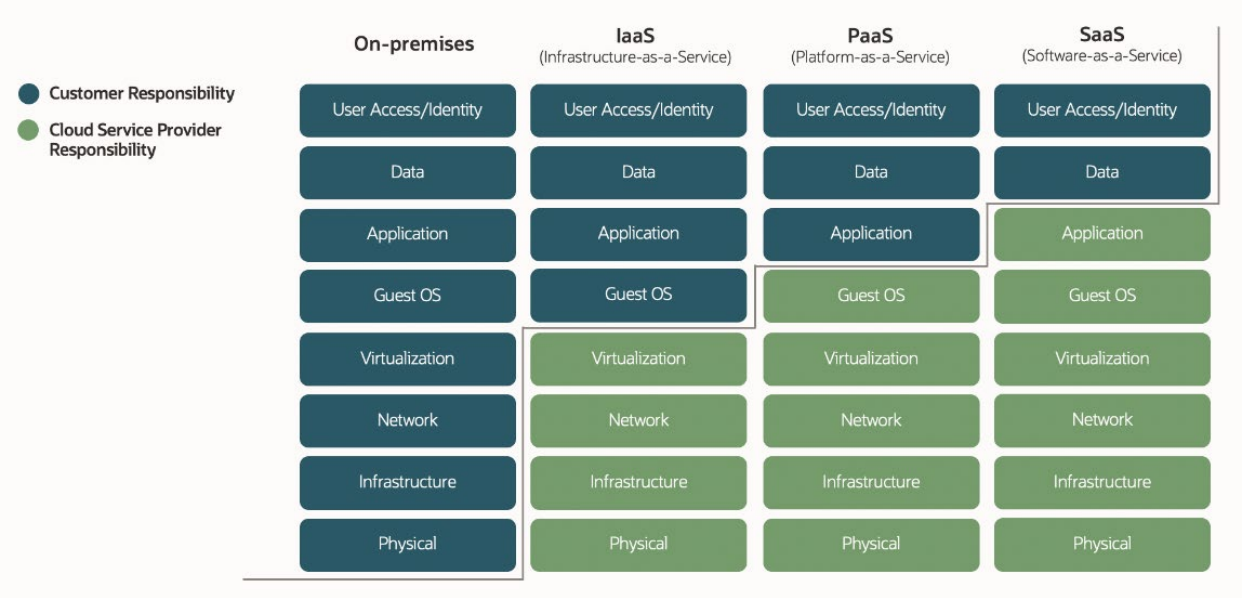

Figure 1: Conceptual Representation of the Various Security Management Responsibilities Between Customers and Cloud Providers

Summary of NERC CIP Standards

Oracle is not regulated by FERC or subject to NERC CIP cybersecurity standards. However, we are committed to helping NERC responsible entities meet their regulatory obligations. Following is a summary of applicable NERC CIP standards and the Oracle practices and controls that may assist responsible entities in evaluating their use of OCI services. NERC CIP compliance, and any determination about the suitability of cloud services in the context of these requirements, is the sole responsibility of the responsible entity.

CIP-003-8—Security Management Controls

NERC requires responsible entities to establish, implement, and maintain cybersecurity policies and procedures. Entities should also document roles and responsibilities related to information security.

Responsible entities are responsible for maintaining all required cybersecurity policies and procedures relevant to their own environment and operations.

Oracle's security policies govern the management of security for both Oracle's internal operations and the systems used in the delivery of services that Oracle provides to its customers. These policies apply to all Oracle personnel, and they are aligned with ISO/IEC 27001:2013 and ISO/IEC 27002:2022 standards. For more information about the Oracle Corporate Security Program, see oracle.com/corporate/security-practices/corporate/governance.html.

CIP-004-6—Personnel & Training

NERC requires responsible entities to implement cybersecurity awareness programs, provide routine training for relevant employees, establish a personnel risk assessment program with background checks, implement access management programs, and establish procedures for revocation upon termination.

Responsible entities are responsible for implementing a formal security awareness program to ensure that their personnel are aware of data security policies and procedures in their own environment.

CIP-005-6 — Electronic Security Perimeter(s)

NERC requires responsible entities to establish network security controls, such as Electronic Security Perimeter (ESP) and Electronic Access Points (EAP), as well as remote access controls such as MFA, encryption, and suspicious activity monitoring.

Responsible entities are responsible for defining, implementing, and enforcing identity and access management policies and procedures with respect to their virtual cloud network, applications, and workloads. Systems should be restricted to their own authorized users.

OCI offers the following services that might help responsible entities meet this requirement:

- **Cloud Guard** helps customers monitor, identify, achieve, and maintain a strong security posture on OCI. This cloud native service examines OCI resources for security weaknesses related to configuration, and OCI operators and users for risky activities. Upon detection, Cloud Guard can suggest, assist with, or take corrective actions, based on the configuration. For more information, see docs.oracle.com/iaas/cloud-guard/home.htm.
- **Vault** key management provides centralized management of the encryption of customer data with keys that customers control. For more information, see docs.oracle.com/iaas/Content/KeyManagement/home.htm.
- **Identity and Access Management (IAM)** lets customers control who has access to cloud resources. Customer can control what type of access a group of users has and to which specific resources. For more information, see docs.oracle.com/iaas/Content/Identity/home1.htm.
- **Virtual cloud networks (VCNs)** give customers complete control over their cloud networking environment, including assigning private IP address spaces, creating subnets and route tables, and configuring stateful firewalls. For more information, see docs.oracle.com/iaas/Content/Network/Concepts/landing.htm.

For more network security documentation, see docs.oracle.com/iaas/Content/Network/Concepts/permissions.htm.

CIP-006-6—Physical Security of BES Cyber Systems

NERC requires responsible entities to establish physical access controls and monitoring, maintain visitor controls and logs, and perform testing on the aforementioned controls.

Responsible entities are responsible for implementing appropriate physical access controls and monitoring that restricts access to sensitive areas and systems in their environment.

Oracle employs measures to prevent unauthorized persons from gaining access to computing facilities in which customer content is hosted. The Oracle Supplier Information and Physical Security Standards outline the ethical, business conduct, and physical security requirements for data centers. These terms apply to vendors who provide data center or colocation services to Oracle for its internal use or for the provision of OCI services to its customers.

CIP-007-6—System Security Management

NERC requires responsible entities enable only necessary physical ports; implement a patch management process; deploy methods to prevent, detect, and mitigate the effects of malicious code; establish processes for monitoring, detection, investigation, and logging of security incidents; and implement system access controls for user authentication and password management.

Responsible entities are responsible for configuring, managing, patching, and maintaining operating systems, databases, applications, and all other components within their environment.

OCI offers the following services that might help responsible entities meet this requirement:

- **Data Safe** is a fully integrated cloud service focused on the security of data. It provides a complete and integrated set of features for protecting sensitive and regulated data in Oracle Cloud databases. Features

include security assessment, user assessment, data discovery, data masking, and activity auditing. For more information, see docs.oracle.com/iaas/data-safe/index.html.

- **Monitoring** helps customers actively and passively monitor their cloud resources by using metrics and alarms that notify them when metrics meet alarm-specific triggers. For more information, see docs.oracle.com/iaas/Content/Monitoring/home.htm.
- **Vulnerability Scanning** helps improve the security posture in an OCI environment when configured to routinely check hosts for potential vulnerabilities. For more information, see docs.oracle.com/iaas/scanning/home.htm.
- **Identity and Access Management (IAM)** lets customers control who has access to cloud resources. Customers can control what type of access a group of users has and to which specific resources. For more information, see docs.oracle.com/iaas/Content/Identity/home1.htm.

OCI maintains a threat and vulnerability management program for the purpose of detecting and remediating vulnerabilities that might affect systems managed by Oracle for the delivery of OCI.

CIP-008-6—Incident Reporting and Response Planning

NERC requires responsible entities to establish incident response plans and to establish processes for implementing, testing, updating, and communicating those plans.

Responsible entities are responsible for implementing an incident response plan for their own environment.

OCI offers the following service that might help responsible entities meet this requirement:

- **Monitoring** helps customers actively and passively monitor their cloud resources by using metrics and alarms that notify them when metrics meet alarm-specific triggers. For more information, see docs.oracle.com/iaas/Content/Monitoring/home.htm.

CIP-009-6—Recovery Plans for BES Cyber Systems

NERC requires responsible entities to establish recovery plans that include conditions for activation, roles and responsibilities, data preservation, and backup. Processes should be established for implementation, testing, updating, and communicating those plans.

Responsible entities are responsible for designing and implementing a cloud architecture that meets their own requirements for availability, business continuity, and disaster recovery.

OCI provides several building blocks that responsible entities can use to plan for the disaster recovery of applications:

- **File Storage** supports snapshots for data protection of file systems. Creating a snapshot of an instance lets customers capture the current state of the nonpersistent boot disk used by an instance. The snapshot can be used to restore a VM. For more information, see docs.oracle.com/iaas/Content/File/Tasks/managingsnapshots.htm.
- **Oracle Active Data Guard** provides data protection and availability for Oracle Databases in a simple and economical manner. It maintains an exact physical replica of the production copy at a remote location that is open read-only while replication is active. For more information, see oracle.com/database/dataguard/.
- **Oracle GoldenGate** is an advanced logical replication product that supports multimaster replication, hub and spoke deployment, and data transformation. GoldenGate provides flexible options to address the complete range of replication requirements, including heterogeneous hardware platforms. For more information, see docs.oracle.com/iaas/goldengate/index.html.

OCI offers recommendations for backup and resilience solutions at docs.oracle.com/en/solutions/oci-best-practices-resilience/index.html.

OCI maintains a Business Impact Analysis (BIA) and Service Resiliency Plan (SRP) for each service. The plans are reviewed annually and include dependencies, roles and responsibilities, and recovery procedures to follow when a service interruption occurs. OCI exercises each service's SRP at least annually.

CIP-010-3—Configuration Change Management and Vulnerability Assessments

NERC requires responsible entities to implement configuration change management processes; establish vulnerability assessment procedures for new and existing information systems, including remediation or mitigation plans for identified vulnerabilities; and manage transient assets and removable media.

Responsible entities are responsible for implementing change management processes in their environment, including, but not limited to, virtual networks, operating systems, virtual machines, databases, storage, and applications.

OCI offers the following service that might help responsible entities meet this requirement:

- **Vulnerability Scanning** helps improve the security posture in an OCI environment when configured to routinely check hosts for potential vulnerabilities. For more information, see docs.oracle.com/iaas/scanning/home.htm.

For Oracle Cloud Services that enable customers to perform maintenance activities, customers are responsible for configuring and maintaining the operating systems and other associated software.

OCI has a comprehensive change management program at the core of its commitment to security, availability, and confidentiality. The process requires changes to be approved and tested before they are implemented. All change requests are documented in an electronic, access-controlled ticketing system. For customer-specific changes and upgrades, where feasible, Oracle coordinates the maintenance periods with customers.

CIP-011-2—Information Protection

NERC requires responsible entities to implement processes and procedures for identifying, protecting, and securely handling (including in storage, during transit, and during use) BES cyber system information, and to establish procedures for reuse and disposal of assets that contain BES cyber system information.

Responsible entities are responsible for designing, developing, testing, implementing, operating, and maintaining administrative and technical safeguards to prevent and detect unauthorized access, use, and disclosure during input, processing, retention, output, and disposition of data to, within, or from their applications.

OCI offers the following services that might help responsible entities meet this requirement:

- **Cloud Guard** helps customers monitor, identify, achieve, and maintain a strong security posture on OCI. This cloud native service examines OCI resources for security weaknesses related to configuration, and OCI operators and users for risky activities. Upon detection, Cloud Guard can suggest, assist with, or take corrective actions, based on the configuration. For more information, see docs.oracle.com/iaas/cloud-guard/home.htm.
- **Vault** is an encryption management service that stores and manages encryption keys and secrets to securely access resources. For more information see, docs.oracle.com/iaas/Content/KeyManagement/home.htm.

Oracle's formal Information Protection Policy establishes requirements for classifying and handling public and confidential information. Oracle categorizes information into four classes—Public, Internal, Restricted, and Highly Restricted—with each classification requiring corresponding levels of security controls, such as encryption requirements for nonpublic data.

Additionally, Oracle's Media Sanitation and Disposal Policy defines requirements for the removal of information from electronic storage media (sanitization) and disposal of information that is no longer required to protect against unauthorized retrieval and reconstruction of confidential data. Electronic storage media include laptops, hard drives, storage devices, and removable media such as tape. The policy also establishes requirements for the removal of information from electronic storage media, including the sanitization and disposal of information to

address scenarios such as end-of-life systems, system repair and reuse, and vendor replacement in conjunction with associated safe data handling. OCI follows National Institute of Standards and Technology (NIST) Special Publication 800-88 Guidelines on Media Sanitization, which addresses ensuring that data is not unintentionally released.

For more information, see the following resources:

- Oracle Corporate Security Practices: oracle.com/corporate/security-practices/corporate/data-protection/
- Oracle Cloud Hosting & Delivery Policies: oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html#hd

CIP-013-1—Supply Chain Risk Management

NERC requires responsible entities to develop and implement a supply chain cybersecurity risk management plan.

Responsible entities are responsible for identifying and assessing environmental, regulatory, and technological changes and, if necessary, updating the design and deployment of their internal controls to ensure the continuing security, availability, and confidentiality of their applications and workloads.

Oracle has formal policies and procedures designed to ensure the safety of its supply chain. These policies and procedures explain how Oracle selects third-party hardware and software that is embedded in Oracle products, as well as how Oracle assesses third-party technology used in Oracle's corporate and cloud environments. Additionally, Oracle has policies and procedures that govern the development, testing, maintenance, and distribution of Oracle software and hardware to mitigate the risks associated with the malicious alteration of these products before purchase and installation by customers.

For more detailed information, see the following resources:

- Oracle Supplier Information and Physical Security Standards: oracle.com/us/corporate/supplier/oracle-supplier-contractor-security-070672.pdf
- Oracle Supplier Security Standards: oracle.com/us/assets/supplier-security-standards-app2-1639575.pdf
- Oracle Supplier Code of Ethics and Business Conduct: oracle.com/webfolder/assets/ebook/supplier-code-of-conduct/index.html#/page/0
- Oracle Supply Chain Security and Assurance Practices: oracle.com/a/ocom/docs/supply-chain-security-assurance-practices.pdf

CIP-014-3—Physical Security

NERC requires responsible entities to periodically conduct and independently verify risk assessments of transmission stations and transmission substations including business impact analysis and identification of primary control centers.

Responsible entities are responsible for conducting risk assessments of their transmission stations and transmission substations and implementing appropriate security controls within their facilities.

Conclusion

NERC responsible entities can use OCI to become more agile, get the in-depth insights that enable them to make business-critical decisions, and reduce costs. Oracle is committed to helping customers operate globally in a fast-changing business environment and meet their regulatory requirements.

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