ORACLE

Hardware Security: Managing Supply Chain Risk In Operations

Document Number and Revision: PROC-10158 Rev 02

Overview

This document is an overview of standards and policies that support the Supply Chain Organization Hardware Security Operations. The listed standards and their related guidelines establish and reinforces the security policies within Oracle Quality Management System (QMS). They are focused on ensuring the integrity and maximizing security of Oracle products through its supply chain.

The standard documents the principles and practices that Oracle customers require adherence to, and the level of quality and efforts expected within the activities. The security agreements we use to manage operations and activities includes but is not limited to Advanced Quality Planning (AQP), NIST, ISO 27001 Information Security, ISO 9000, FedRamp High and Oracle Compliance per the Master Sale Agreement (MSA).

Audience

This document is for Oracle Supply Chain - e.g. Supplier Sourcing Managers, Program Management, OHD Management, Engineering, OCI as well as EMs to Oracle, JDMs, and Oracle's Sub-tier Suppliers.

Table of Contents

1.0 Introduction

This document provides security and quality management standards whose purpose include the description, activities and methods used to protect the integrity of the hardware shipping to OCI Data Centers and to on-prem customers. These standards and guidelines are not intended to substitute the existing Oracle security policies but build upon them. The development, implementation, approaches, and administrative procedures that support the Hardware Security operations objective are encompassed within the standards. Together these standards, policies and guidelines provide the methods employed to ensure consistency amongst the operational activities conducted across the Supply Chain Organization (SCO).

2.0 Types of Suppliers

Reference the Advanced Quality Planning (AQP) matrix specification 913-3592 for the full list of supplier definitions.

Example below:

External Manufacturer (EM) - Contract Manufacturer (Oracle classifies these vendors as an EM) - An organization that makes products under a legal agreement with the customer. Contract manufacturers generally serve the Original Equipment Manufacturing (OEM) market.

3.0 Hardware Security Program

Through the security standards we aim to equip SCO with the tools and framework necessary to meet ongoing Compliance, Government Security requirements and successful fulfillment of customer demand. By creating a consistent framework across supply chains and manufacturing models from NPI through EOSL, we handle the responsibility for outsource suppliers and manufacturer.

It is crucial as suppliers are introduced, developed and managed that we maintain the highest level of security. Communication to hardware security can vary e.g., adding a new supplier to the AML, custom delays, logistics, Oracle

Intellectual destruction (e.g., Root of Trust (RoT), supplier recyclers) Tamper Evident Packaging, hardware counterfeit, hardware security risk surveys, hardware theft, piloting a hardware program, physical security audits, NPI development with a new EM, NCATs and data center hardware incidents.

Key questions centered around the program.

- Is the hardware secure? Where are the gaps in our supply chain?
- Are we prepared for the unexpected? E.g., Physical Security Attack, Supply Chain Security interruptions, Pandemic, Data Leak, Environmental hazards, etc

Compliance Checklist:

- Is this a new supplier?
- Has formal agreement been reached between Oracle and the supplier?
- Verified the supplier has the latest AQP 913-3592 document and the spec's tied to the AQP?
- Is the supplier going to use Tamper evident packaging?
- Will this supplier handle high value assets?
- Has the supplier verified Customs-Trade Partnership Against Terrorism (C-TPAT) certification?

4.0 Hardware Security Framework

We evolve our operational practices to ever changing regulations and challenges that the security environment presents. With advancement in technology, increased adoption of cloud-based services, and rise in Cybersecurity attacks, it's critical organizations improve security tactics and have strong security controls in place. This guide is intended to provide fundamental principles of Hardware Supply Chain Security Risk Management, help establish better approaches for monitoring operational processes for incident detention, improve response to and recovery from a security incident and point the reader to more detailed documents, as appropriate. The hardware security framework consists of:

- Customer Requirement
- Oracle's Supplier Information and Physical Security Standards
- National Standards - NIST and FedRAMP High
- Advanced Quality Planning (AQP)
- International Standards - ISO 9001 Quality Management System (QMS) and ISO 27001 Information Security Management Systems (ISMS)

4.1 Physical Hardware Security Requirements

Oracle has implemented industry best practices to mitigate supply chain risk across its direct hardware supply chain as well as Oracle suppliers. These practices include, but are not limited to, data security, physical security, supply chain and product security. Oracle requests its suppliers to comply with Oracle's Supplier Information and Physical Security Standards, which define these practices.

These Supplier Information and Physical Security Standards contain security controls that cover:

- Handling Oracle confidential information;
- Custody of Oracle hardware assets.

The above Supplier Information and Physical Security Standards (the "Standards") also specifically address the following security controls:

- Appendix 1: Supply Chain Physical Security;
- Appendix 2: Supplier Data Center Security;
- Appendix 3: Source Code Protection and Secure Development.

Supplier is responsible for compliance with these standards by its personnel and subcontractors, including ensuring all personnel and subcontractors are bound by contractual terms consistent with the requirements of these Standards. Additional security compliance requirements may be specified in Supplier's agreement or individual statements of work.

4.1.2 High Value Asset (HVA)

Hardware Security is committed to identifying and prioritizing High Value Assets (HVAs) and assessing the security surrounding HVAs. Through continuous review we protect the information and hardware. HVAs may contain sensitive instructions and data used in critical operations. Unauthorized access, use, modification, or destruction of HVAs can cause a significant impact to the confidence and integrity of the hardware. To counter threats to the security of HVAs, all items identified as an HVA require enhanced security controls by all involved in the manufacturing, procurement, and handling process.

The categories in identifying HVAs include: Information Value and Business Essential

If the hardware can perform the primary functions which include providing instructions, communicating, decode, execute, store data and provide the processing power for the hardware to do its work (be read to or written to) then it is considered to be an option for high value. E.g., PDU, PSU, NICs (Host/Smart), RoT, CPU, Motherboards and select FRUs are examples.

The high value asset list is designated by Oracle requirements and therefore is subject to change based on customer or Line of Business (LOB) requirements.

If you are unsure about the HVA requirements or require additional information, contact: scosecurityrequest_us_grp@oracle.com or SLACK #SCOhardware_security_risk_gov

4.1.3 Specification for Handling High Value Asset (HVA)

The procedure and requirements for handling HVAs are within AQP spec PROC-10090 Physical Security, Control, Traceability, and Destruction of Supply Chain High Value Assets at External Manufacturers and Suppliers.

4.2 Hardware Security Audit

The objective of the hardware security audit is to gather sufficient and appropriate evidence in order to validate suppliers and their sub-tiers compliance with the applicable criteria (e.g., MSA, AQP, NIST, FedRAMP High, ISO, applicable laws, regulations and contract terms) and to support the hardware security auditor compliance determination.

The nature and extent of audits will depend upon Oracle agreement, suppliers' size and the amount and type of business. The hardware security audits can be used to support the assessment of control risk for other related audits (e.g., quality management, logistics, proposals, sub-tier management reviews, etc) to determine the degree of reliance that can be placed on suppliers' systems and controls as a basic for operational planning.

In the cases where the suppliers' findings include outstanding and major operational system deficiencies, the hardware security auditor will recommend actions to correct the deficiencies (e.g., supplier scorecard failure, disapproval of system, failure of audit, suspension of production, etc)

For audit questions, please slack #SCOhardware_security_risk_gov or send an email to: scosecurityrequest_us_grp@oracle.com

4.2.1 National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) provides a collection of best practices to help businesses to understand, manage, reduce security risk and protect their data. The standards provide controls to ensure measurement traceability, enable quality assurance, and harmonize documentary standards and regulatory practices.

By adopting the NIST framework, hardware security can leverage the controls, focus on the supply chain security risk as it applies to information sharing, procurement, manufacturing lifecycle and identify the gaps within the organization's operational practices.

4.2.2 ISO 9001 – Quality Management System (QMS)

ISO 9001 is defined as the international standard that specifies requirements for a quality management system (QMS). It is the most popular standard in the ISO 9000 family series. Organizations use the standard to demonstrate the ability to consistently provide products and services that meet customer and regulatory requirements.

Source: https://www.iso.org/iso-9001-quality-management.html

4.2.3 ISO 27001 – Information Security Management Systems (ISMS)

ISO 27001 is defined as the international standard that specifies requirements for a ISMS. ISO/IEC 27001 promotes a holistic approach to information security: vetting people, policies and technology. Its founding principles focuses on three aspects of information: confidentiality, Integrity and availability of the information. An information security management system implemented according to this standard is a tool for risk management, cyber-resilience and operational excellence.

Source: https://www.iso.org/standard/27001

4.2.4 FedRamp High

The Federal Risk and Authorization Management (FedRamp) is a government-wide program that promotes the use of modern cloud technology and requires cloud providers to protect federal information. Oracle is certified FedRamp High and as part of the mandatory requirements for government customers strict security controls must be administered. The program is based off principles on providing standardized framework to protect data confidentiality, integrity, risk assessment, authorization and continuous monitoring for cloud products and services.

Source: https://www.oracle.com/industries/government/govcloud/fedramp-high-jab/

4.2.5 Advanced Quality Planning (AQP)

The Advanced Quality Planning Specifications are a set of quality and supply chain related requirements bindings to suppliers. They are presented in a table called the “AQP Matrix” spec 913-3592 and included in the contractual obligations. Oracle’s suppliers are audited to the specifications for compliance. The AQP Matrix can be located in AQP secure sites and in Fusion Product Development (PD).

The AQP matrix covers a wide range variety of Oracle processes from design through shipment, as well as applicable relevant industry and government standards. Suppliers know which specifications they must comply with by checking the Xs in their assigned supplier type column on the matrix. Furthermore, the AQP is referenced in Oracle Contracts with the external manufacturer. Notifications of changes are sent to suppliers when an AQP document is updated. Suppliers have a 30-day window to object to the changes. After 30 days the supplier is expected to fully implement and comply with the change. If the supplier does not contest or object to the change the Supplier is deemed to have agreed to comply with the changes to the AQP document.

5.0 Chain of Custody: Security in Transportation

What is Chain of Custody?

"A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer." The key process is following your supply chain through its lifecycle.

Examples of assets include equipment, infrastructure, evidence, systems, and data. Maintaining the chain of custody increases transparency and enables accountability for actions taken on the asset. In practice, chain-of-custody documentation can support risk mitigation by reducing the opportunity for malicious actors to tamper with the asset (e.g., equipment, data, or evidence)

Source: NIST SP 800-72 under Chain of Custody

5.1 Tamper Evident Labeling and Packaging

Oracle has introduced tamper evident packaging as an additional layer of defense against supply chain transportation risks. The requirements are defined within the 8218708 Tamper Evident Packaging specification. Reference the document in the AQP matrix for the latest revision.

The purpose of these techniques is not to make packages look inconspicuous. The purpose is to detect tampering with the equipment and material being shipped to all Oracle customers (commercial and government).

5.1.1 Security Requirements for Tamper Evident Packaging Materials

All Tamper Evident Packaging material (i.e., seals/labels, bands and clear rack bags) require enhanced security controls by all involved in the manufacturing, procurement and handling process.

Henceforth, all Tamper Evident Packaging material shall be securely locked and stored during non-production hours i.e., such as end of shift, during breaks and close of business. Physical inventory count shall be frequently done for inventory management and verification.

Oracle Manufacturing and Oracle EMs shall request approval through scosecurityrequest_us_grp@oracle.com prior to the destruction of Tamper Evident Packaging material. Reference specification 8218708 for Tamper Evident Packaging requirements.

5.2 Potential Impacts of a Broken Chain of Custody

The integrity of the system and its underlying data/equipment can no longer be trusted.
The reliability, accuracy, and security of records in question – physical or digital – cannot be guaranteed. All Hardware Security chain of custody events are investigated, and hardware systematically reviewed to assess security impact.

6.0 Destruction Process

Reference specification PROC-10090 Physical Security, Control, Tracebility and Destruction of Supply Chain High Value Assets at External Manufacturers and Suppliers.

7.0 Traceability

Oracle must have the ability to rapidly locate, contain, and replace suspect material throughout the Supply Chain. This capability is referred to as traceability. Oracle requires suppliers to provide product traceability data for products containing Oracle part numbers (PNs) to an Oracle data repository. This gives Oracle the traceability to enable rapid location, containment, and replacement of suspect material throughout its supply chain and the product life cycle (PLC).

7.1 Non-Conformance Corrective Action Tool (NCAT)

The NCAT is SCO's formal Root Cause Corrective Action (RCCA) tool and is part of the key performance indicator (KPI) hardware security measures suppliers against for risk management.

7.2 Counterfeit Detection

Counterfeit material contains unauthorized reproduction or alterations misrepresented to be authentic, used material represented as new with false identification (e.g., lot codes, serial number, date code, material performance, hidden cosmetic defects etc). Oracle reduces the likelihood of unauthorized modifications at each stage in the supply chain and protects information systems and information system components prior to taking delivery of such systems/components by employing preemptive supply chain agreements that obligate our suppliers to Oracle specifications, and subsequent audits as laid out in Oracle's Advance Quality Planning (AQP) specification matrix.

Suppliers are required to implement counterfeit avoidance processes/system to know the source and detect or mitigate unauthorized material from entering its supply chain. Measures to mitigate counterfeit material can include but not limited to documenting inspection process, appropriate testing, training and bringing awareness to sub-tiers, all or necessary departments involved within the supply chain.

Supplier Agreements

Our Master Supply Agreement (MSA) and/or Master Purchase and Service Agreements contains exhibits that obligate our suppliers to specific authentic material or component requirements. Those requirements:

Obligates Oracle's supplier to only acquire Oracle materials by either developing and manufacturing Oracle parts as authorized by Oracle, utilizing an authorized subtier supplier, and/or by utilizing Oracle's most current approved supplier list.

Obligates Oracle's supplier to refrain from and prevent subtier suppliers from any activity deemed as unauthorized use, unauthorized distribution, or misuse of Oracle products.

Obligates Oracle's supplier to refrain from and prevent subtier suppliers from activities that constitute counterfeiting, unauthorized gray market, and/or any other unauthorized activities from involving Oracle products.

Stipulates that Oracle's supplier must have preventative programs in place to prevent and deter activities mentioned above.

8.0 Information Protection of Oracle Data

The following guidelines represent best practices that are useful in fulfilling the goals of the hardware security standard. We encourage you to verify and properly label all communication. Reference Oracle Supplier Information and Physical Security Standards.

- Internal and external communication must be properly labeled with confidentiality marking
- Meeting minutes - Awareness of data that should be on a "need to know" basis
- CUI – Classified Uncontrolled Information (Identifiable information, both digital and physical, created by a government (or an entity on its behalf) that, while not classified, is still sensitive and requires protection.)
- E.g., Technical information, technical drawings or blueprints, MFG part, Components, Spec details, manual, financial statements, contracts, engineered data, imagery intelligence, source code. Not Commercial Off the Shelf (COTS)

The sample above is intended to provide an example of a script that may risk hardware security. By following practices and procedures designed to foster decision making responsible partiees can help protect information systems and the data that supports the mission. E.g., All company documents should be safeguarded. When sharing, utilize password protection and SecureSites.

9.0 Contact

SCO QMS	E-mail
Advanced Quality Planning (AQP) & Traceability	christine.bump@oracle.com
Customer Audits/Escalations	michelle.gordon@oracle.com
Non-Conforming Corrective Action Tool (NCAT)	michelle.gordon@oracle.com, paul.pfeffer@oracle.com, jonathan.masters@oracle.com
OCI Corrective Action Preventive Action (CAPA)	michelle.gordon@oracle.com
Product Quality Management (PQM)	jonathan.masters@oracle.com
SCO Quality Management System (QMS)	paul.pfeffer@oracle.com
Stop Ship and Purge (SSP)	jonathan.masters@oracle.com

HW Security Risk Management	E-mail
Business Continuity Plan (BCP)	michelle.gordon@oracle.com, sabrina.zaman@oracle.com
NIST/FedRAMP High	michelle.gordon@oracle.com,

	sabrina.zaman@oracle.com, wes.beausoleil@oracle.com
SCO Compliance/Hardware Security/External Manufacturer Audits	michelle.gordon@oracle.com,sabrina.zaman@oracle.com, wes.beausoleil@oralce.com
High Value Asset (HVA) Traceability/Incident Investigation	christine.bump@oracle.com

For questions, please slack #SCOhardware_security_risk_gov or send an email to: scosecurityrequest_us_grp@oracle.com

10.0 Glossary

Classified Information	Information that has been identified and require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
Confidentiality	Involves the protection of identifiable data from unauthorized disclosures and access
Integrity	Integrity refers to the security or protection of information from unauthorized access or revision. Integrity ensures that the information is not compromised through malicious, unintentional/intentional attacks.
Information Security	means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service; the potential for a threat source to successfully exploit a particular information system vulnerability.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

11.0 FAQ's

1. How does Oracle prevent counterfeit items/parts from entering our supply chain?

Our supply chain agreements obligate our suppliers to Oracle specifications, and subsequent audits as laid out in Oracle's Advance Quality Planning (AQP) specification matrix. See counterfeit detections for additional details.

12.0 Documents to Reference

- *913-3592, Manufacturing/Operations Requirements Advanced Quality Planning (AQP) Matrix*
- *923-3406, Supplier Traceability Requirements*
- *7326396, Supplier Traceability Data, CSV Data Feed Format*
- *923-2349, Sub-Tier Supplier Management Roles and Responsibilities*
- *923-1826 Stop Ship and Purge (SSP) Process for Hardware Products*
- *923-3644 Corrective and Preventive Action Process*
- *8218708 Specification for Tamper Evident Packaging*
- *PROC-10090 Oracle Supply Chain High Value Asset Physical Security, Control, Traceability and Destruction Process*
- *Oracle Supplier Information and Physical Security Standards* https://www.oracle.com/us/assets/oracle-supplier-contractor-security-070672.pdf

13.0 Revision History

REV	DATE	DESCRIPTION OF CHANGE	CHANGE ORIGINATOR
02	01/18/2024	Initial Release	N/A

- When Document Template is complete, email source file to eso_business_docs_us_grp@oracle.com
- **All hard copies of this document are uncontrolled and are to be used for reference only.**
- For questions or comments about this document, please slack or send an email to:

  Slack #SCOhardware_security_risk_gov or send an email to scosecurityrequest_us_grp@oracle.com