ORACLE
PUBLIC SECTOR

Oracle Public Sector Compliance Overview

Common compliance topics explained

ORACLE WHITE PAPER | FEBRUARY 2015

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, functionality, or certification or compliance status, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Table of Contents

Introduction

Some Public Sector customers have unique security and compliance concerns that they target to meet in regards to the confidentiality, integrity, and availability of their information, and sometimes the requirements of various government compliance programs can be complex and difficult to navigate. This whitepaper provides a ***high-level overview*** and ***general explanation*** for Oracle's intended compliance with Public Sector requirements, and is formatted in a similar structure to the list of control requirements specified by the National Institute of Standards and Technologies (NIST) Special Publication 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations". Furthermore, as NIST 800-53 requirements are directly relational to standards established by the International Organization for Standardization (ISO), this whitepaper can also be used to explain potential compliance in the context of International secure computing standards.

Oracle Public Sector Cloud employs management controls, operational controls, and technical controls generally aligned with the security framework of the United States Federal Risk and Authorization Management Program (FedRAMP), The National Institute for Standards and Technologies (NIST), International Organization for Standardization (ISO) and Code of Practice for Information Security Management. For Oracle, targeting adherence to Federal and International security standards are the foundation of our secure Public Sector Cloud practice.

Oracle security practices and procedures are internal-only and are not generally shared outside of Oracle without a signed NDA. For questions regarding specific descriptions of Oracle security measures or to review Oracle policies please contact an Oracle Public Sector sales representative.

FedRAMP and Data Categorization Overview

The FedRAMP program acts as a cloud broker by accrediting cloud service providers (CSP's) and facilitating the procurement of cloud services for state, local and federal government agencies. FedRAMP has three basic categories of cloud service providers (or CSP) based on security level:

- "Low" indicates a lower threshold of security compliance and is aimed at serving the needs of government customers who have less strict security requirements
- "Moderate" indicates a moderate security threshold and is aimed at customers who require a variety of security requirements in order to protect more sensitive data
- "High" is an accreditation level that is still in development by the General Services Administration (GSA). If and when this security level is defined and announced it will indicate a high security threshold that requires compliance with a very wide variety of security requirements. This level is aimed at serving customers with very restricted and sensitive security requirements.

The standard that FedRAMP uses to assess and accredit CSP's is a publication provided by NIST called the ***NIST Special Publication 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations".*** This is a large publication which provides a variety of security requirements that CSP's are required to deploy. NIST provides these standards as a baseline; additionally, FedRAMP uses all of the NIST standards and adds some additional

requirements for compliance. Thus, CSP's that meet Low or Moderate levels as accredited by FedRAMP, are also considered meeting all of the requirements for a Low or Moderate level accreditation as defined by NIST 800-53, with additional requirements added by FedRAMP.

In order to help customers understand which level of cloud security is right for them, NIST published a guide that assists cloud users with classifying the security needs of their data. This guide is called the Federal Information Processing Standard (FIPS) 199 "Standards for Security Categorization of Federal Information and Information Systems". Also, as required by FedRAMP, CSP's evaluate their systems according to the FIPS 199 publication in order to verify the level of data that their environment can accommodate.

Security Requirements specified by NIST SP 800-53

The current NIST 800-53 contains groups of requirements called "Control Families". Currently there are 17 control families:

- Access Control
- Awareness and Training
- Audit and Accountability
- Certification, Accreditation, and Security Assessment
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity

Each control family contains a list (or family) of related security requirements. For example, the control family called "Access Control" has a list of requirements that are all related to access control.

Below is a high-level summary of Oracle's policies and how they may apply to each control family of the NIST SP 800-53 security requirements. Note that Oracle maintains many policies that might be applicable to each Control Family, but described are only the *primary* policy (or policies) that most directly relates to each Control Family.

Oracle Organizational Security Overview

Oracle's Information Security Strategy includes a risk-based approach for addressing information security, designed to facilitate protection of Oracle's information and information entrusted to Oracle.

This approach is designed to enable Oracle's Global Information Security team, a delegated entity (such as an Information Security Manager, ISM), or a Line of Business, to focus on critical

information security areas where risk management process can be brought to bear to reduce, remove, transfer or accept identified and rated risks.

Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls are contained in the Information Security Policy. Oracle generally follows an assessment procedure as described in the Information Security Policy, with additional guidance from NIST SP 800-30 and NIST SP 800-37. This process outlines how the assessment should be conducted in order to implement controls at the NIST 800-53 Moderate baseline. Oracle has gone through the C&A process and security assessments with an independent, third-party assessor, and with various customers.

The Chief Corporate Architect, who reports directly to the Executive Chairman of the Board and Chief Technology Officer, manages the functional departments directly responsible for identifying and implementing security controls at Oracle. The Global Information Security, Global Product Security, Global Physical Security, and Oracle Security Architecture organizations comprise Oracle Corporate Security, which provides independent security policy, guidance and compliance oversight to Oracle worldwide.

Oracle also has virtual team structures to provide business units with resources to address information security areas of specialty. These include a Security Oversight Committee that provides direction and senior management support for security initiatives at Oracle, Information Privacy and Regulatory Compliance teams, and Information Security Managers and Information Owners in key lines of business.

Oracle Security Oversight Committee: The OSOC is a cross functional team of senior management representatives from key organizations within Oracle. The OSOC recommends, reviews, and approves security strategy decisions and security initiatives at Oracle.

Global Information Security: Global Information Security (GIS) is responsible for security oversight, compliance, enforcement, conducting information security assessments, leading the development of information security policy and strategy, as well as training and awareness at the corporate level. GIS serves as the primary contact for security incident response, providing overall direction for incident prevention, identification, investigation, and resolution.

Product Development IT (PDIT) Cloud Security and Compliance: PDIT Cloud Security and Compliance is responsible for IT security strategy, architectural design of security solutions, engineering, risk management, security infrastructure operations and support, standards and compliance, threat intelligence and remediation, and security technical assessment for new infrastructure across the cloud operations organization. PDIT Cloud Security and Compliance also facilitates audits, including customer and third party compliance reviews.

Oracle Policies Relating to NIST 800-53 Control Families

Access Control

Oracle's approach to access control is described in the *Oracle Logical Access Control Policy* and the *Oracle Single Sign-On Policy.*

The Oracle *Logical Access Controls Policy* describes logical access control requirements for Oracle systems, including authentication, authorization, access approval, provisioning, and revocation for employees and any other Oracle-defined users with access to Oracle systems which are not Internet-facing, publicly accessible systems.

The Oracle *Single Sign-on Policy* describes the use of a centralized source for user authentication and identity management for web based applications. Personnel accessing the Oracle Public Sector Cloud and Oracle Public Sector Cloud application components are required to first have a Single Sign-On (SSO) account. All SSO access and account control are strictly controlled and documented in practice documents associated with the SSO Policy.

Audit and Accountability

The *Oracle Logging and Log Analysis Policy* describes Oracle's approach to audit and accountability.

The objective of the Oracle *Logging and Log Analysis Policy* is to ensure accountability of all relevant actions on a system and to require regular monitoring and timely response to security incidents such as unauthorized access or unauthorized use of data or programs. Specific standards must be created at the application, database, host (operating system), and network device level.

The Oracle *Logging and Log Analysis Policy* states Oracle's corporate-level mandates for log retention, review, and analysis. Areas covered include minimum log requirements, responsibilities for the configuration and implementation of logging, alert review, problem management, retention, security and protection of logs, as well as compliance review.

Awareness and Training

Oracle's Security Awareness and Training Policy and Procedures are described in the *Oracle Employee Handbook*, the *Oracle Information Security Policy,* the *Oracle Employee Code of Ethics and Business Conduct* and the *Oracle Acceptable Use Policy.*

The *Oracle Employee Handbook* specifies many mandatory aspects of employee training, including security training. Information security awareness and training resources, including mandatory courses, are made available to Oracle users and personnel with security-related duties and responsibilities, to ensure they are aware of the risks and vulnerabilities associated with their activities; the relevant and applicable legislative, regulatory and contractual requirements; and have the training necessary to carry out their responsibilities.

The *Oracle Information Security Policy* describes the principles for development, executive approval, implementation, and maintenance of information security policies and practices at Oracle. This over-arching information security policy also describes governing principles such as

'need to know', Least Privilege, and segregation of duties; employees, contractors and temporary employees are subject to the Information Security Policy.

The Oracle *Code of Ethics and Business Conduct* sets forth Oracle's high standards for moral ethics and business conduct at every level of the organization, and at every location where Oracle does business throughout the world. The standard applies to Oracle employees, independent contractors, and temporary employees; it covers areas of Oracle's legal and regulatory compliance and business conduct and relationships. Compliance-tracked training in ethics and business conduct and sensitive information handling is required once every two years.

The *Oracle Acceptable Use Policy for Company Resources* sets requirements for use of the Oracle corporate network, computer systems, telephony systems, messaging technologies, Internet access, and other company resources.

Certification, Accreditation, and Security Assessment

Oracle's security assessment and authorization policy is set forth in the *Oracle Information Security Policy*, the *Oracle Information Security Risk Assessment Methodology Handbook* and the *Oracle Security Organization Policy*.

The Oracle *Information Security Policy* describes the principles for development, executive approval, implementation, and maintenance of all information security policies and practices at Oracle. This over-arching information security policy also describes governing principles such as 'need to know', Least Privilege, and segregation of duties. All employees, contractors and temporary employees are subject to the *Information Security Policy*.

The *Information Security Risk Assessment Methodology (or ISRAM) Handbook* is a handbook-style guide which describes Oracle's scalable model for determining Information Security risk associated with Oracle's business. The ISRAM constitutes one methodology, but two approaches:

- a more comprehensive approach which is suited to detailed risk assessments
- a general approach which is used for more basic and quicker assessment process

The *Oracle Security Organization Policy* describes and clarifies the roles and responsibilities of various teams and individuals involved in information security at Oracle, including the executive-level Oversight Committee, Corporate Information, Product, and Physical Security organizations, IT and IT Security organizations, all Lines of Business (LoBs) and individual Information Security Managers (ISMs) who are assigned by each LoB to represent the security leadership of each organization.

Oracle and our third-party auditors submit a variety of documentation that is required as part of certification, accreditation and security assessment process as defined by FedRAMP. This documentation currently includes:

- A System Security Plan (or SSP) which is used to provide a detailed description of the security posture of an IT system being accredited by FedRAMP
- A System Assessment Plan (or SAP) which is used by third-party auditors as a plan for security testing of FedRAMP applicants
- A System Assessment Report (or SAR) which is used to provide guidance on the implementation of security requirements
- A Plan of Action & Milestones (or POA&M) which is used to provide a structured approach to risk mitigation and audit remediation

For more information on these reports please refer to the FedRAMP website at https://cloud.cio.gov/fedramp.

Oracle Cloud currently employs accredited third parties to conduct independent reviews of the service offering in the following areas:

- FedRAMP compliance
- ISO 27001 compliance
- DoD ECSB Cloud Security Model compliance
- Statement on Standards for Attestation Engagements (SSAE) No16, Service Organization Control (SOC) 1 & 2 reports. Scope of reporting may vary by service and country
- Other independent third party security testing to review the compliance and effectiveness of administrative, operational, technical, management, and physical controls

Not all of these may be available for all Cloud offerings. Available reports may be provided to Oracle Cloud customers upon written request. Please contact an Oracle sales representative for assistance.

Configuration Management

Oracle's oversight of Change Management is described in the *Oracle Security Organization Policy.*

The *Oracle Security Organization Policy* describes and clarifies the roles and responsibilities of various teams and individuals involved in information security at Oracle, including the executive-level Oversight Committee, Corporate Information, Product, and Physical Security organizations, IT and IT Security organizations, all lines of business (LoB's) and individual Information Security Managers (ISMs) who are assigned by each LoB to represent the security leadership of each organization. This policy includes a description of the key stakeholders involved with aspects of change management, including the adherence to other documents critical to change management, specifically the *Oracle Enterprise Hosting & Delivery Policies* and the *Oracle Cloud Configuration Management Plan.*

Contingency Planning

Oracle's Contingency Planning policies and procedures are set forth in the *Oracle Risk Management & Resiliency Policy* and managed by the *Oracle Risk Management and Resiliency Program.*

The *Oracle Risk Management & Resiliency Policy* describes the management of risk assessment, contingency planning and testing, employee awareness, and auditing of Oracle systems.

The *Oracle Risk Management and Resiliency Program (RMRP).* The objective of this program is to implement the policy specified in the Oracle Risk Management & Resiliency Policy.

Identification and Authentication

Oracle's Identification and Authentication policy is set forth in *the Oracle Logical Access Control Policy*, and the *Oracle Single Sign-On Policy*, and the *Oracle Password Policy*.

The *Oracle Logical Access Controls Policy* describes logical access control requirements for Oracle systems, including authentication, authorization, access approval, provisioning, and

revocation for employees and any other Oracle-defined users with access to Oracle systems which are not Internet-facing, publicly accessible systems.

The *Oracle Single Sign-on Policy* describes the use of a centralized source for user authentication and identity management for web based applications. Personnel accessing the Oracle Public Sector Cloud and Oracle Public Sector Cloud application components are required to first have a Single Sign-On (SSO) account. All SSO access and account control are strictly controlled and thoroughly documented in practice documents associated with the SSO Policy.

The Oracle *Password Policy* requires effective protection of information assets by Oracle employee use of strong password controls where passwords are being used as a method of authentication.

Incident Response

Oracle's Incident Response policy and procedures is set forth in the *Oracle Information Security Incident Reporting and Response Policy,* the *Oracle Incident Response Plan* and the *Oracle Security Breach Disclosure Policy*.

The Oracle *Information Security Incident Reporting and Response Policy* requires reporting of and response to information security incidents in a timely and efficient manner. Oracle also maintains a detailed Information Security Incident Response Plan to provide specific guidance for personnel involved in or supporting incident response.

The Oracle *Security Breach Disclosure Policy* provides requirements for Oracle employees to notify identified contacts internally in the event of suspected unauthorized access to PII. In accordance with the *Oracle Security Breach Disclosure Policy* Oracle employees must immediately bring any suspected security incidents of this nature to the attention of the Legal Department and Global Information Security.

Maintenance

Oracle's System Maintenance policy and procedures is set forth in the *Oracle Cloud Enterprise Hosting and Delivery Policies*

Per the *Oracle Cloud Enterprise Hosting and Delivery Policies*, Oracle may periodically deploy Oracle patches, maintenance releases, and updates to the customer's services environment to keep the Oracle programs provided by Oracle as part of the services at a current release version or to enhance service performance. The Enterprise Hosting and Delivery Policies include descriptions of the following:

- Oracle Cloud Change Management and Maintenance
- Application Upgrades and Updates
- Core System Maintenance
- Routine Infrastructure Maintenance

Media Protection

Oracle's sanitization policy is set forth in the *Oracle Media Sanitization and Disposal Policy* and the *Oracle Cloud Enterprise Hosting and Delivery Policies.*

The Oracle *Media Sanitization and Disposal Policy* establishes guidelines for secure erasure of information from different types of electronic media, where current usage of the media is finished and a decision has to be made regarding recycling or destruction. The policy is intended to protect Oracle resources and information from security threats associated with the retrieval and recovery of information on electronic media.

The *Oracle Cloud Enterprise Hosting and Delivery Policies* provides additional information regarding physical media transport and data disposal. Specifically, the *Oracle Cloud Enterprise Hosting and Delivery Policies* addresses the methodology of secure physical medial transport, data disposal, and other media protection topics.

*Note: The unauthorized use of removable, optical, and external media (to include output devices such as printers) is **strictly prohibited** in the Oracle Public Sector Cloud data center environment.*

Personnel Security

Oracle's Security Awareness and Training Policy and Procedures are set forth in the *Oracle Information Security Policy*, the *Oracle Employee Code of Ethics and Business Conduct* and the *Oracle Acceptable Use Policy*.

The Oracle *Information Security Policy* describes the principles for development, executive approval, implementation, and maintenance of information security policies and practices at Oracle. This over-arching information security policy also describes governing principles such as 'need to know', Least Privilege, and segregation of duties. Employees, contractors and temporary employees are subject to the *Information Security Policy*.

The Oracle *Code of Ethics and Business Conduct* sets forth Oracle's high standards for moral ethics and business conduct at every level of the organization, and at every location where Oracle does business throughout the world. The standard applies to Oracle employees, independent contractors, and temporary employees; it covers the areas of legal and regulatory compliance and business conduct and relationships. Compliance-tracked training in ethics and business conduct and sensitive information handling is required once every two years.

The *Oracle Acceptable Use Policy for Company Resources* sets requirements for use of the Oracle corporate network, computer systems, telephony systems, messaging technologies, Internet access, and other company resources.

Physical and Environmental Protection

Oracle's Physical and Environmental Protection policy and procedures is set forth in *Oracle Supplier Information and Physical Security Standards*, the *Oracle Information Protection Policy*.

The *Supplier Information and Physical Security Standards* provides a comprehensive and structured approach to information and physical security. This set of standards applies to the assets, information and systems accessed by Oracle suppliers. The *Oracle Supplier Information and Physical Security Standards* provides a list of the security controls that Oracle's Suppliers are required to adopt when (a) accessing Oracle or Oracle customer facilities, networks,

environments and/or confidential information, or (b) having custody of products or assets. Oracle suppliers are responsible for compliance with these standards by its personnel, including ensuring that all supplier personnel are bound by contractual terms consistent with the requirements of the standards.

The Oracle *Information Protection Policy* provides guidelines for all Oracle personnel regarding information classification schemes and minimum handling requirements associated with those classifications in an effort to ensure protection of Oracle and Customer information assets.

Planning

Oracle's Security Planning Policy and Procedures is set forth in *Oracle Information Security Policy*.

The Oracle *Information Security Policy* describes the principles for development, executive approval, implementation, and maintenance of all information security policies and practices at Oracle. This over-arching information security policy also describes governing principles such as 'need to know', Least Privilege, and segregation of duties. Employees, contractors and temporary employees are subject to the *Information Security Policy*.

Risk Assessment

Oracle's Risk Assessment policy and procedures is set forth in the *Oracle Information Security Policy* and the *Oracle Information Security Risk Assessment Methodology Handbook*.

The Oracle *Information Security Policy* describes the principles for development, executive approval, implementation, and maintenance of all information security policies and practices at Oracle. This over-arching information security policy also describes governing principles such as 'need to know', Least Privilege, and segregation of duties. Employees, contractors and temporary employees are subject to the *Information Security Policy*.

The *Information Security Risk Assessment Methodology (or ISRAM) Handbook* is a handbook-style guide which describes Oracle's scalable model for determining Information Security risk associated with Oracle's business. The ISRAM constitutes one methodology, but two approaches:

- a more comprehensive approach which is suited to detailed risk assessments
- a general approach which is used for more basic and quicker assessment process

System & Information Integrity

Oracle's System & Information Integrity policy is set forth in the *Oracle Information Security Policy* and the *Oracle Server Security Policy*.

The Oracle *Information Security Policy* describes the principles for development, executive approval, implementation, and maintenance of all information security policies and practices at Oracle. This over-arching information security policy also describes governing principles such as 'need to know', Least Privilege, and segregation of duties. Employees, contractors and temporary employees are subject to the *Information Security Policy*.

The Oracle *Server Security Policy* sets forth the physical and logical security requirements for Internet-facing and production Servers. This policy requires servers owned and managed by

Oracle ("servers") to be physically and logically secured so as to prevent unauthorized external access to the servers and the information assets they hold and process.

System & Services Acquisition

Oracle's Services and Systems Acquisitions policy and procedures is described in the *Oracle Supplier Information and Physical Security Standards*.

The *Supplier Information and Physical Security Standards* provides a comprehensive and structured approach to information and physical security when acquiring systems and services. This comprehensive approach includes managing security of Oracle's assets, information and systems accessed by its Suppliers. The *Oracle Supplier Information and Physical Security Standards* provides a list of the security controls that Oracle's Suppliers are required to adopt when (a) accessing Oracle or Oracle customer facilities, networks, environments and/or confidential information, or (b) having custody of products or assets. Oracle suppliers are responsible for compliance with these standards by its personnel, including ensuring that all supplier personnel are bound by contractual terms consistent with the requirements of the standards.

Systems & Communications Protection

Oracle's Systems and Communications Protections policy and procedures is set forth in the *Oracle Network Security Policy.*

The purpose of the *Oracle Network Security Policy* is to provide official guidance related to: the protection of information assets, the management of interconnectivity with Oracle systems, and the protection of Oracle's networked resources. The *Oracle Network Security Policy* applies to Oracle users as well as all network devices.

More information about Oracle Security Policies

Oracle Security Policy Review Process

Oracle Cloud information security policies establish and govern areas of security applicable to Oracle Cloud services and to its customers' use of Oracle Cloud services. Oracle personnel (including employees, contractors, and temporary employees) are subject to Oracle Cloud security policies and any additional policies that govern their employment or the services they provide to Oracle. Oracle Cloud information security policies and documentation may be reviewed at the sole discretion of Oracle management. Changes and updates to any policy will be made in accordance with the *Oracle Policy Review Process.* Policy revisions may be carried out either following an annual review or as and when required depending on the factors that necessitate revisions. Following approval by Oracle Security Oversight Committee (OSOC), new Global Information Security (GIS) policies, and policies that have been subject to version changes, are formally implemented in accordance with the *Oracle Policy Roll-Out Process.*

Security Responsibilities of Oracle Customers

Oracle Cloud customers are responsible for:

- Implementing their own comprehensive system of security and operational policies, standards and procedures, according to their risk-based assessments and business requirements.
- Ensuring that end-user devices meet web browser requirements and minimum network bandwidth requirements for access to their Oracle Cloud environment.
- Managing client device security controls, for example so that antivirus/malware checks are performed on data or files before importing or uploading data into their Oracle Cloud environment.
- Maintaining customer-managed accounts according to customer policies and security best practices.

Each customer is responsible for all End User administration within the subscribed service or application. Oracle does not manage the Customer's End User accounts. Customer may be able to configure the applications and additional built-in security features.

For each customer site (i.e., for each agency), Oracle creates an administrator account to be used by the agency for administration of the application. The individual filling this administrator role is responsible for managing accounts for authorized agency users and ensuring that those accounts comply with the agency's security requirements.
Each customer is responsible for ensuring that adequate account management processes are in place and that all users are appropriately verified and issued unique user IDs. The Oracle Public Sector Cloud requires customer site administrators to assign unique IDs to all users.

Customers may not perform network scans, vulnerability scans, or penetration tests on the Oracle Public Sector Cloud environment. If a customer has a regulatory requirement for such tests, then the customer can submit a service request (SR) that is forwarded to the appropriate security teams at Oracle for review on a case-by-case basis.

References:

Policies:

Oracle Cloud Enterprise Hosting and Delivery Policies
Oracle Information Security Policy
Oracle Information Protection Policy
Oracle Acceptable Use Policy
Oracle Server Security Policy
Oracle Media Sanitization and Disposal Policy
Oracle Information Security Incident Reporting and Response Policy
Oracle Security Breach Disclosure Policy
Oracle Risk Management & Resiliency Policy
Oracle Logical Access Control Policy
Oracle Single Sign-On Policy

Standards:

Oracle Supplier Information and Physical Security Standards
Oracle Global Media Sanitization and Disposal Security Standard

Processes:

Oracle Policy Review Process
Oracle Policy Roll-Out Process

Other Info:

Oracle Employee Code of Conduct

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US


blogs.oracle.com/oracle


facebook.com/oracle


twitter.com/oracle


oracle.com

Hardware and Software, Engineered to Work Together


Oracle is committed to developing practices and products that help protect the environment