Advisory: Oracle Cloud Infrastructure and Good Practice (GxP) Guidelines

Description of Oracle Cloud Infrastructure Practices, Controls, and Features in the Context of US FDA 21 CFR Part 11 Subpart B and EudraLex, Volume 4, Annex 11

November 2022 Version 2.0

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 in assessing your use of Oracle Cloud Infrastructure (OCI) in the context of the requirements applicable to you under the Good Practice (GxP) guidelines, including FDA 21 CFR Part 11 Subpart B and EudraLex, Volume 4, Annex 11. This document might also help you to assess Oracle as an outsourced service provider. You remain responsible for independently assessing 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 remain at the sole discretion of Oracle.

FDA 21 CFR Part 11 Subpart B and EudraLex, Volume 4, Annex 11 are subject to periodic changes or revisions by their respective regulatory authorities, the US Food & Drug Administration (FDA) and the European Medicines Agency (EMA). The FDA 21 CFR Part 11 Subpart B regulations are available at ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11/subpart-B?toc=1. The EudraLex, Volume 4, Annex 11 guidelines are available at ec.europa.eu/health/medicinal-products/eudralex/eudralex-volume-4_en.

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.

Contents

Introduction

The Good Practice (GxP) guidelines are intended to ensure that food, medical devices, drugs, and other life science products are safe, while maintaining the quality of processes throughout every stage of manufacturing, control, storage, and distribution. GxP guidelines are produced by regulatory authorities such as the Food & Drug Administration (FDA) in the US and the European Medicines Agency (EMA) in the EU. GxP encompasses several regulatory guidelines, but the most common are Good Clinical Practices (GCP), Good Laboratory Practices (GLP), and Good Manufacturing Practices (GMP).

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 in relation to FDA 21 CFR Part 11 Subpart B and EudraLex, Volume 4, Annex 11.

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.

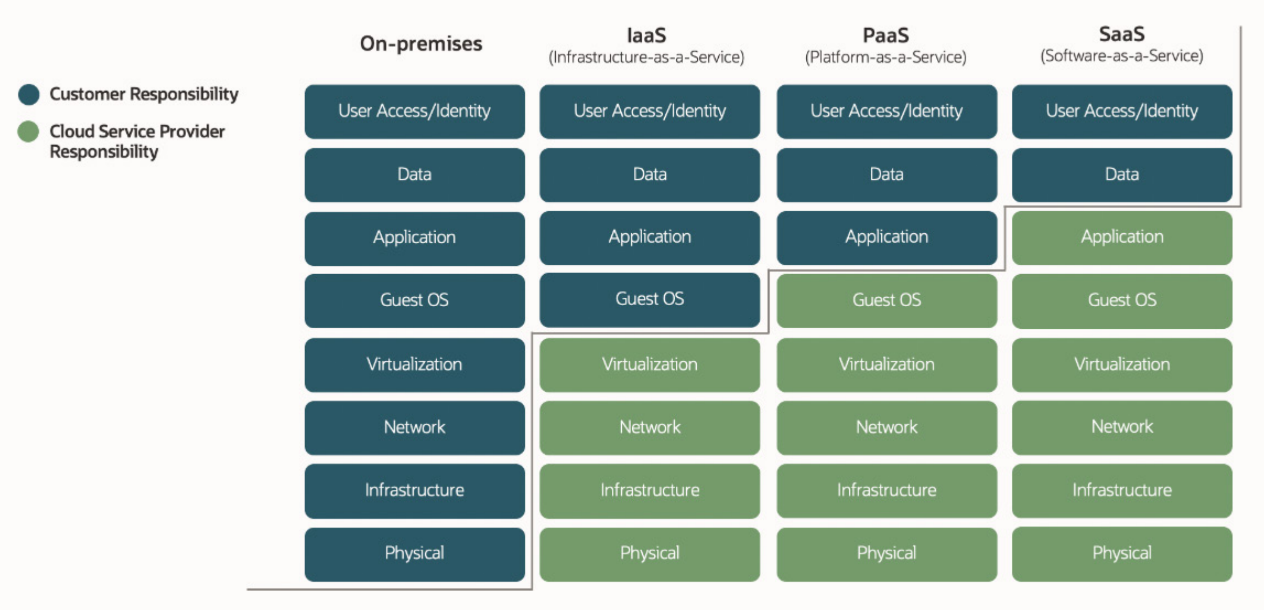

Figure 1: Conceptual Representation of the Various Security Management Responsibilities Between Customers and Cloud Providers

Summary of FDA 21 CFR Part 11 Subpart B and EudraLex, Volume 4, Annex 11

This section describes key considerations for customers using OCI for their GxP applications and workloads. Customers are solely responsible for determining the suitability of cloud services in the context of FDA 21 CFR Part 11 Subpart B and EudraLex, Volume 4, Annex 11. Organizations deploying systems on OCI are responsible for determining the GxP requirements that apply to their systems, based on the intended use and regulatory standard.

FDA 21 CFR Part 11 Subpart B – Electronic Records

The following table details key considerations for customers running their FDA-regulated computerized systems or applications on OCI. This information includes a brief summary of customer responsibilities, OCI standards and controls, and OCI services and features that might help customers meet their obligations under FDA 21 CFR Part 11 Subpart B, 11.10 Controls for close systems.

CFR RULE REFERENCE	CFR CONTROL AREA	IMPLEMENTATION
11.10	Persons who use closed systems to create, modify, maintain or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	
11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Customers using OCI products in FDA-regulated systems are fully responsible for all software-validation activities. Oracle has implemented practices and controls to help ensure that its infrastructure and platform services are built and tested to meet industry security, reliability, and quality standards. OCI has been assessed against global compliance standards including SOC, ISO, and FedRAMP. For more information, see Oracle Cloud Compliance at oracle.com/corporate/cloud-compliance/. OCI supports reliability and consistent performance with its data regions located within specific geographies. Each data region has one, two, or three availability domains, and each availability domain is split into multiple fault domains. Whether a customer instance resides in a region with one availability domain or multiple available domains, numerous layers of redundancy are available for data and service resiliency and backups through fault domains and cross-region replication. OCI provides the services and documentation needed to build and run applications in a highly secure, hosted environment with high performance and availability. For more information, see docs.oracle.com/en/solutions/oci-best-practices/reliable-and-resilient-cloud-topology-practices1.html.
11.10 (b)	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	Customers are responsible for maintaining the accuracy and completeness of their electronic records, and for the direct protection of their data and applications. As a cloud infrastructure provider, OCI generally has no insight into the data that customers store or process in OCI. Oracle has no ability to generate copies of these records. Customers can use OCI services such as Audit, which records calls to OCI public API endpoints as log events, and Logging, which provides logs from OCI resources, including how they are performing and being accessed.
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Customers are responsible for implementing security procedures that protect against unauthorized access or changes to their systems and data. Oracle has implemented controls to help ensure that data is stored and maintained securely. For example, OCI tenant data is encrypted at rest and in transit. Data storage services, such as Block Volume and Object Storage enable at-rest data encryption by default by using the Advanced Encryption Standard (AES) algorithm with 256-bit encryption. In-transit control plane data is encrypted using Transport Layer Security (TLS) 1.2 or later. Customers can implement data backups as part of a resilient architecture to align with their record retention policies. For more information, see docs.oracle.com/en/solutions/oci-best-practices/back-your-data1.html.

CFR RULE REFERENCE	CFR CONTROL AREA	IMPLEMENTATION
11.10 (d)	Limiting system access to authorized individuals.	Customers are responsible for the direct protection of their data and applications, including implementing security procedures that protect against unauthorized access to their systems and data. Customers can use OCI services such as Identity and Access Management to implement access management features for OCI and applications, and Vault key-management services to store and manage encryption keys. OCI has implemented controls to help ensure that access to the infrastructure is limited to authorized individuals. Access to infrastructure and services that support the system requires multifactor authentication (MFA), a VPN connection, and an SSH connection with a user account and password or private key. OCI account creation, access approval, access grant, and access review are based on the principles of least privilege, need to know, and segregation of duties.
11.10 (e)	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	Customers are responsible for all aspects of system data retention and integrity, which should be considered in the design and development of computerized systems. These responsibilities include implementing audit controls within the customer's environment and logging of development history events or data changes. Customers may use OCI services such as Audit, which records calls to OCI public API endpoints as log events that can be exported and retained based on customer retention requirements, and Logging, which provides logs from OCI resources, including how they are performing and being accessed. OCI services must record all logs in accordance with the Oracle Logging and Log Analysis Policy. OCI services store audit logs using a high-availability system that is protected to help ensure validity and integrity.
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	This control area is not applicable to OCI. Customers are responsible for configuring, establishing, and verifying enforcement of permitted sequencing steps and events within their environments.
11.10 (g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	This control is not applicable to OCI. Customers are responsible for designing, developing, testing, implementing, operating, and maintaining administrative and technical safeguards to prevent or detect unauthorized access, use, and disclosure during input, processing, retention, output, and disposition of data to, within, or from their applications.
11.10 (h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	This control is not applicable to OCI. Customers are responsible for the data hosted in OCI, including verifying the validity of the source of data.
11.10 (i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	This control is not applicable to OCI. Customers are responsible for implementing a formal screening, training, and education program to help ensure that personnel have the knowledge and experience required to meet GxP requirements in their environment.

CFR RULE REFERENCE	CFR CONTROL AREA	IMPLEMENTATION
11.10 (j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	This control is not applicable to OCI. Customers are responsible for establishing and enforcing their own internal policies and procedures to hold their employees or other users accountable and responsible for their individual actions.
11.10 (k)	Use of appropriate controls over systems documentation including:	
11.10 (k) (1)	Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	Customers are responsible for implementing and managing procedural controls that govern the access to and use of system documentation within their environment. OCI provides documentation for the use and management of cloud tenancies. For more information, see docs.oracle.com/iaas/Content/cloud-adoption-framework/management-and-operations.htm. Oracle maintains documented procedural controls to manage the access and use of system documentation for the OCI environment.
11.10 (k) (2)	Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Customers are responsible for changes made to their own systems, including the maintenance of appropriate documentation and change management procedures. OCI has implemented and documented a rigorous change-management process in its PaaS and IaaS environments. Changes to infrastructure configurations and services that support the system are documented in an electronic, access-controlled ticketing system. The ticketing system captures information regarding the nature of the proposed change, impact, required updates to system documentation, test plan, notification plan, rollback plan, and postimplementation verification. All changes deployed in OCI production environments follow a peer review, testing, and approval process before implementation. Planned maintenance notifications are communicated to the customer through the Oracle Cloud Console. For more information, see the Oracle Cloud Change Management Policy in the Oracle Cloud Hosting and Delivery Policies at oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf.

EudraLex, Volume 4, Annex 11: Computerized Systems

The following table details key considerations for customers running their medicinal products regulated by the European Commission on computerized systems and/or applications on OCI. This information includes a brief summary of customer responsibilities, OCI practices and controls, and OCI services and features that might help customers meet their obligations under the EudraLex, Volume 4 Good Manufacturing Practice (GMP), Annex 11 Computerized Systems guidelines.

PRINCIPLE	GUIDANCE	IMPLEMENTATION
1. Risk Management	Risk management should be applied throughout the lifecycle of the computerized system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerized system.	Customers are responsible for identifying and assessing environmental, regulatory, and technological changes and, if necessary, updating the design and deployment of its internal controls to help ensure the continuing security, availability, and confidentiality of their applications and workloads. However, Oracle has implemented protective measures for identifying, analyzing, measuring, mitigating, responding to, and monitoring risk specific to its cloud services organizations. Risk assessments are performed annually across Oracle Cloud services to identify threats and risks that could impact the security, confidentiality, or availability of the system. Risks are reviewed, assigned an owner, and remediated in line with the Oracle Cloud services risk management assessment program.
2. Personnel	There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	Customers are responsible for implementing a formal training, and education program to help ensure that personnel have the knowledge and experience required to meet GxP requirements in their environment. Customers are responsible for establishing and enforcing their own internal policies and procedures to hold their employees or other users accountable and responsible for their individual actions. Customers should maintain records of personnel qualifications and training and, where applicable, disciplinary or corrective actions. For information about OCI training and certification, see education.oracle.com/learn/oracle-cloud-infrastructure/pPillar_640. **Note**: Oracle employees are assigned a job description when they are hired that defines their role and the necessary qualifications for their position. Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, security, operation, maintenance, and monitoring of the system. OCI's Quality Management System consists of policies, requirements, and procedures to help ensure that records of appropriate compliance training, staff education, and experience for all positions are maintained.
3. Suppliers and Service Providers		
3.1	When third parties (e.g., suppliers, service providers) are used e.g., to provide, install, configure, integrate, validate, maintain (e.g., via remote access), modify or retain a computerized system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party.	Customers are responsible for ensuring that they have formal, written agreements with all third parties (for example, suppliers and service providers) that clearly define the roles of each party. Contracts between Oracle and its customers set out the rights and obligations of each party, and are executed before the provision of cloud services. Oracle Cloud Service Contracts are available at oracle.com/corporate/contracts/cloud-services/contracts.html. Oracle maintains formal, written agreements with all third parties (for example, suppliers and service providers) that it uses. These

PRINCIPLE	GUIDANCE	IMPLEMENTATION
		agreements set out the requirements that suppliers and service providers are required to adhere to. For information about Oracle Supply Chain Security and Assurance, see oracle.com/corporate/security-practices/corporate/supply-chain/.
3.2	The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.	Customers are responsible for identifying and assessing the competence and reliability of their suppliers based on their system requirements and risk assessment. Oracle has published several documents to assist its customers in conducting necessary risk assessments and due diligence. Oracle provides customers with the Cloud Security Alliance Consensus Assessment Initiative Questionnaire (CAIQ), audit reports, and other information regarding Oracle's operational and security practices: • Oracle Cloud Compliance: oracle.com/corporate/cloud-compliance/ • Oracle Cloud CAIQs: oracle.com/corporate/security-practices/cloud/ • Cloud Services Hosting and Delivery Policies: oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html • Oracle Corporate Security Practices: oracle.com/corporate/security-practices/
3.3	Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.	Customers are responsible for developing and maintaining an appropriate quality-management system of their suppliers and their suppliers' products and services. This system should include procedures for risk assessments and quality audits.
3.4	Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.	Customers are responsible for developing and maintaining an appropriate quality-management system of their suppliers and their suppliers' products and services. This system should include procedures for risk assessments and quality audits. OCI maintains a quality-management system to help ensure that OCI services and features help enable the customer to meet security, availability, confidentiality, and integrity requirements. OCI's quality-management system is audited by an independent third party and certified in accordance with ISO 9001 standards.
4. Validation		
4.1	The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.	Customers are responsible for all system-validation documentation of their GxP systems, including protocols, acceptance criteria, and procedures.
4.2	Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.	Customers are responsible for all system-validation documentation and testing of their GxP systems, including change control records.
4.3	An up to date listing of all relevant systems and their GMP functionality (inventory) should be available.	Customers are responsible for all system-validation documentation of their GxP systems, including relevant system inventory.

PRINCIPLE	GUIDANCE	IMPLEMENTATION
4.4	User Requirements Specifications should describe the required functions of the computerized system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.	Customers are responsible for all system-validation documentation of their GxP systems, including user requirement specifications.
4.5	The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.	Customers are responsible for all system-validation documentation and testing of their GxP systems, including the implementation of an appropriate quality-management system.
4.6	For the validation of bespoke or customized computerized systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.	Customers are responsible for all system-validation documentation and testing of their GxP systems, including the assessment and reporting of quality and performance measures.
4.7	Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.	Customers are responsible for all system-validation documentation and testing of their GxP systems, including system parameter limits, data limits, and error handling.
4.8	If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.	Customers are responsible for all system-validation documentation and testing of their GxP systems, including data-integrity checks.
5. Data	Computerized systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.	Customers are responsible for the direct protection of their data and applications, including implementing appropriate security controls for secure processing of data. Customers are responsible for encrypting data in transit within their on-premises environment. As cloud provider, Oracle generally has no insight into the data that customers store or process in OCI. However, to help meet this requirement, customers can use OCI services such as Block Volume, Object Storage, and File Storage, which encrypt data at rest using AES 256-bit encryption, and Vault, which manages keys and secrets.
6. Accuracy Checks	For critical data entered manually, there should be an additional check on the accuracy of the data. This check maybe done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.	Customers are responsible for ensuring that appropriate checks are in place to validate the accuracy of source data entered into their GxP systems. As cloud provider, Oracle generally has no insight into the data that customers store or process in OCI, or the accuracy of such data.

PRINCIPLE	GUIDANCE	IMPLEMENTATION
7. Data Storage		
7.1	Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability, and accuracy. Access to data should be ensured throughout the retention period.	Customers are responsible for directly protecting their data and applications, including implementing security measures that restrict access to their own facilities and locations where they operate. This responsibility includes physically securing access to and transmission of data, and restricting the display of data, to authorized individuals. To help meet this requirement, customers can use OCI services such as Block Volume, Object Storage, Archive Storage, and File Storage, which encrypt data at rest by using AES 256-bit encryption.
7.2	Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.	Customers are responsible for implementing a backup process, a replication process, or both in line with their requirements and policies. To help meet this requirement, customers can use OCI services such as Block Volume and Object Storage, and the Oracle Database Cloud Backup Module. **Note**: The Oracle Cloud Hosting and Delivery Policies describe the Oracle Cloud Services Backup Strategy. The PaaS and IaaS Public Cloud Services Pillar Document provides more information about specific cloud services. See oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html.
8. Printouts		
8.1	It should be possible to obtain clear printed copies of electronically stored data.	Customers are responsible for ensuring that printed copies of electronically stored data are available.
8.2	For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.	Customers are responsible for the integrity and accuracy of data generated, stored, or processed by their systems.
9. Audit Trails	Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated “audit trail”). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.	Customers are solely responsible for meeting this requirement. As cloud provider, Oracle generally has no insight into the data that customers store or process in OCI, or whether the data has been altered. However, to help meet this requirement, customers can use OCI services such as Audit and Logging.
10. Change and Configuration Management	Any changes to a computerized system including system configurations should only be made in a controlled manner in accordance with a defined procedure.	Customers are responsible for any changes made to their environment, including, but not limited to, virtual networks, operating systems, virtual machines, databases, storage, and applications. However, changes to infrastructure configurations and services that support the system follow the Cloud Compliance Standard for Change Management. They are documented in an access-controlled ticketing system, tested, and peer-reviewed before implementation. The Oracle Change Management Policy, including roles and responsibilities, is detailed in the Oracle Cloud Hosting and Deliveries Policy at oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html.

PRINCIPLE	GUIDANCE	IMPLEMENTATION
11. Periodic Evaluation	Computerized systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.	Customers are responsible for periodically evaluating computerized systems in their environment and complying with GMP requirements. Periodic evaluation of computerized systems in the context of GMP is not applicable to OCI. However, OCI infrastructure and platform services are subject to independent third-party audits no less than annually. OCI evaluates and communicates internal control findings in a timely manner to those parties responsible for taking corrective action. Findings are reviewed and tracked through resolution.
12. Security		
12.1	Physical and/or logical controls should be in place to restrict access to computerized system to authorized persons. Suitable methods of preventing unauthorized entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.	Customers are responsible for directly protecting their data and applications. This protection includes physical and logical security measures that restrict access to its own facilities, systems, and data from unauthorized individuals. To help meet this requirement, customers can use OCI services such as Vault and Security Zones. However, Oracle physical and environmental security controls restrict access to OCI data halls within colocation facilities, its own premises, and other locations where it operates. The Oracle Supplier Information and Physical Security Standard outlines the business conduct and physical security requirements for data center vendors. See oracle.com/assets/supplier-security-standards-app2-1639575.pdf.
12.2	The extent of security controls depends on the criticality of the computerized system.	Customers are responsible for determining the criticality of their systems and implementing appropriate controls. OCI has implemented physical and logical security controls to provide a highly secure, hosted environment with high performance and availability. For more detailed information about OCI security controls, see the OCI SOC 2 Type 2 Report.
12.3	Creation, change, and cancellation of access authorizations should be recorded.	Customers are responsible for implementing logical and physical access management policies and procedures in their environment, and for recording changes in access status. The Oracle Cloud Standard for Access Control defines the parameters for who can create, change, and terminate Oracle access logs. OCI services maintain a record of the following events: user access is provisioned, privileges are granted, application transactions are performed, and access to the application is modified or terminated.
12.4	Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.	Customers are responsible for restricting access to confidential information stored or processed in their applications and workloads to authorized parties, in accordance with their confidentiality commitments and requirements. Customers shall implement the appropriate processes and procedures for access management, including access logs and monitoring.
13. Incident Management	All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.	Customers are responsible for implementing incident-management plans in their systems. Incident-management procedures for reporting and tracking incidents and implementing corrective and preventative actions should be documented and tested no less than annually. OCI has implemented a Corrective Action Preventive Action (CAPA) program to review all incidents after resolution and identify the root cause of failures, effectiveness of resolutions, and preventative

PRINCIPLE	GUIDANCE	IMPLEMENTATION
		actions that can be implemented. Product security defects and vulnerabilities are assessed by cross-functional teams, including personnel from the Global Information Security (GIS) and Global Product Security (GPS) functions. OCI security incidents are assigned a severity rating and tracked to resolution by the OCI Detection and Response Team (DART). OCI reports confirmed security incidents with customer impact to Oracle GIS and Oracle Legal, who are responsible for any notices or disclosures to the public, customers, affected individuals, or law enforcement authorities.
14. Electronic Signature	Electronic records may be signed electronically. Electronic signatures are expected to: a. have the same impact as hand-written signatures within the boundaries of the company, b. be permanently linked to their respective record, c. include the time and date that they were applied.	Customers are responsible for maintaining all electronic records and implementing electronic signature policies and procedures to meet this requirement.
15. Batch Release	When a computerized system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.	Customers are responsible for all certification activities as it relates to batch releases and qualified personnel.
16. Business Continuity	For the availability of computerized systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g., a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.	Customers are responsible for designing and implementing a cloud architecture that meets their own requirements for availability, business continuity, and disaster recovery. Learn about the disaster recovery capabilities of Oracle Cloud at docs.oracle.com/en/solutions/design-dr/. OCI maintains a Business Impact Analysis (BIA) and Service Resiliency Plan (SRP) for each service. The plans are reviewed annually and include an assigned owner, documented roles and responsibilities, detailed recovery procedures and reference information, and the method for plan invocation. Learn more about Oracle's Risk Management Resiliency Program at oracle.com/corporate/security-practices/corporate/resilience-management/business-continuity.html.
17. Archiving	Data may be archived. This data should be checked for accessibility, readability, and integrity. If relevant changes are to be made to the system (e.g., computer equipment or programs), then the ability to retrieve the data should be ensured and tested.	Customers are responsible for architecting, implementing, and testing a data archive strategy to meet their requirements. As cloud provider, Oracle generally has no insight into the data that customers store or process in OCI. However, to help meet this requirement, customers can use OCI services such as Block Volume and Object Storage, and the Oracle Database Cloud Backup Module.

Conclusion

Organizations operating in the life sciences industry face stringent regulatory requirements to ensure the safety and efficacy of biotechnology, pharmaceutical, and medical device products. OCI provides a collection of complementary cloud platform and infrastructure services that enables customers to build a run a wide range of applications and services in a highly available hosted environment. In addition, OCI provides a number of tools and capabilities that can help life science organizations meet the technical requirements associated with their regulatory obligations.

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