ORACLE

ADVISORY: ORACLE LIFE SCIENCES CLOUD SERVICES AND "GXP" GUIDELINES

Description of Good Practices "GxP" Guidelines and Requirements in relation to Oracle Life Sciences Cloud Services Practices and Controls

September 2023, Version 1.0

Public

Disclaimer

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

This document is for informational purposes only and is intended solely to assist you assessing your use of Oracle cloud services in the context of the requirements applicable to you under the Good Practice (GxP) guidelines, including but not limited to the FDA 21 CFR Part 11 Subpart B and EudraLex, Volume 4, and Annex 11. This may also help you to assess Oracle as an outsourced service provider. You remain responsible for making your own independent assessment of the information in this document as the information in this document 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 upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

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. The EudraLex, Volume 4, Annex 11 guidelines are available at ec.europa.eu.

This document is based upon information available at the time of drafting. It is subject to change at the sole discretion of Oracle Corporation and may not always reflect changes in the regulations

Introduction

The Good Practice (GxP) guidelines and regulations comprise a set of global guidelines for traceability, accountability and data integrity. They are intended to ensure 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. Some of the primary regulators include Food & Drug Administration (FDA) in the US, Therapeutic Goods Administration (TGA) in Australia, and Health Canada | Santé Canada (HC-SC) in Canada, European Medicines Agency (EMA) and National Medical Products Agency (NMPA) in China. GxP includes varied regulation sets, but the most common are GCP, GLP, and GMP. For more information, see https://www.fda.gov/drugs/guidance-compliance-regulatory-information.

This document is intended to assist GxP regulated organizations with their assessment and utilization of OLS Cloud Services.

Document Purpose

This document is intended to provide relevant information related to OLS Cloud Services for clinical research and vigilance and to assist you in determining the suitability of using OLS Cloud Services in relation to GxP. The information contained in this document does not constitute legal advice. Regulated organizations are advised to seek their own legal counsel to develop and implement their compliance program and to assess the features and functionality provided by OLS in regard to their specific legal and regulatory requirements.

The list of clinical research and vigilance products for OLS Cloud Services associated with this paper is provided at https://www.oracle.com/life-sciences/products

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 with regard to their specific legal and regulatory requirements.

About Oracle Life Sciences

OLS Cloud Service offerings combine the elasticity and utility of the cloud with the control, security, high performance delivery, high-availability and cost-effective Infrastructure associated with Software as a Service (SaaS). OLS recognizes the GxP regulatory requirements regulated organizations must follow and we are committed in supporting our customers to address their GxP obligations.

SaaS, a cloud-based software delivery model, is the world's most complete, connected SaaS suite. Oracle manages the hardware and traditional software, including middleware, application and software security so our customers can deploy, scale and upgrade business solutions more quickly.

OLS provides industry leading solutions to regulated organizations including pharmaceutical and medical device companies, Contract Research Organizations (CROs) and Academic Research Organizations (AROs) for over 15 years. The OLS Cloud Services portfolio includes cloud solutions such as study start-up activities, study management, data management, analytics and trial consulting services.

Table of contents

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 environments. By design, Oracle provides security functions for cloud infrastructure and operations (e.g., cloud operator access controls, infrastructure security patching), and customers are responsible for securely configuring and using their cloud resources. For more information, you should refer to your cloud service documentation.

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

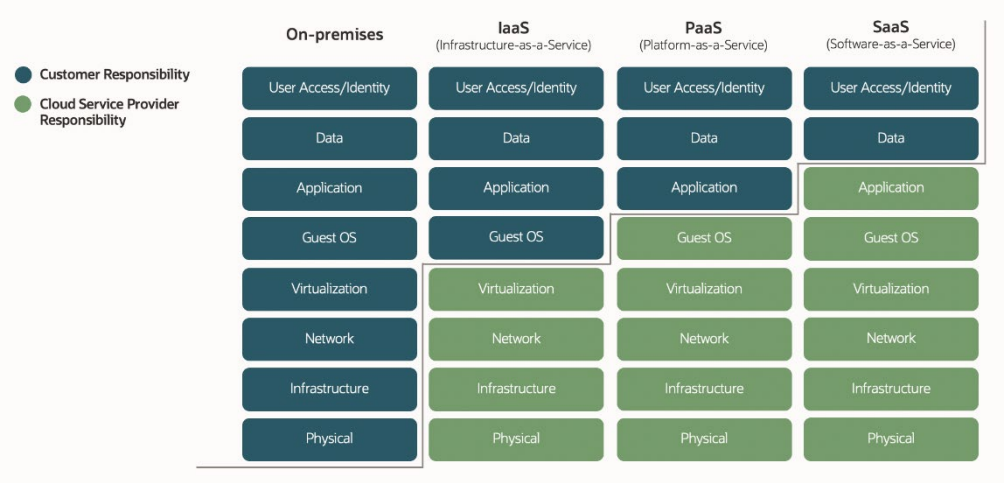


Figure 1: Conceptual representation of the various security management responsibilities between customers and cloud providers

Customer Responsibilities

Regulated organizations are solely responsible for determining the suitability of cloud services in the context of their regulatory requirements. As illustrated in Figure 1 above, regulated organizations are responsible for the data brought into the Cloud Services (including its classification, handling and retention requirements) together with any associated user access/identity activities (including the specification of roles and permissions).

When OLS Cloud Services are integrated with regulated organization managed applications running on OCI or other customer environments the regulated organizations need to remain aware of their responsibility for the validation of environments receiving data from or transmitting data to the OLS Cloud Service. Overall accountability for assuring the validated status of computerized systems in use for clinical trial or vigilance purposes is the regulated organizations responsibility.

COMPLIANCE FRAMEWORK

Global regulatory entities (e.g. FDA, MHRA, etc) do not provide GxP certification to cloud service providers in the delivery of services for clinical trials, investigations or drug and device safety.

OLS makes available a range of documentation to support a regulated organization's use of Oracle cloud services including independent third-party certificates and attestation reports addressing compliance frameworks for both OLS Cloud Services and associated OCI services. Through System and Organization Controls Level 2 (SOC 2) type 2 attestation reports, and ISO/IEC 20000-1, 27001, 27017, 27018, 27701, and 9001 certifications, OCI has evidenced the implementation of security controls in protecting the confidentiality, integrity, and availability of information assets in the OCI environments.

Controls are verified, through independent third-party assessments conducted on a quarterly, semi-annual or annual basis.

Click the following links for further information on Oracle Cloud Compliance, and our OCI and Good Practice (GxP) Guideline on our Advisory page.

System and Organization Controls (SOC)

System and Organization Control (SOC) reports are a standardised industry approach to independently assessing the effectiveness of an organization's controls for financial reporting (SOC1) or operational controls (SOC2) relating to the security, availability, processing integrity, confidentiality and privacy of data processed as part of a service delivery. SOC1 or SOC2 Reports consist of two types: Type 1 reports discuss the suitability of the design of applicable controls for their stated control objectives at a certain time point whereas Type 2 reports consider the suitability of the design of the applicable controls and their operating effectiveness over a particular time period. SOC Reports are prepared by an independent third-party on a semi-annual basis for various components developed on and utilizing OLS OCI, which helps to support OLS Cloud Services.

International Organization for Standardization (ISO)

The International Organization for Standardization, ISO is a non-governmental organization, founded in 1946, with membership comprised of national standards bodies. ISO standards such as the ISO/IEC 2700 series (which encompass information security, cybersecurity, and privacy protection) may be prepared in conjunction with the International Electrotechnical Commission, IEC. The ISO 9000 series of standards addresses quality management and quality assurance.

OLS Cloud Services undergo annual certification through third-party audits against the ISO/IEC 27001 and 27018 standards, security and privacy controls for product development, application management and product support. The OLS quality management system (QMS) has attained ISO 9001:2015 certification.

Oracle Cloud Infrastructure security and privacy controls have also been separately certified against ISO/IEC 27001, 27017 and 27018.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a US federal law that established data privacy and security requirements for certain entities and individuals aimed at safeguarding individuals' health information. HIPAA mandates privacy and security protections for protected health information (PHI) and applies to individuals and entities meeting said definition. The original HIPAA requirements have been augmented through additional legislation specifically the HIPAA Privacy Rule, HIPAA Security Rule, HITECH Act and Omnibus Rule.

OCI regions and services are in-scope for bi-annual HIPAA assessments. For more information, please see the following link to the HIPAA Assessed Regions and Services page: https://www.oracle.com/cloud/cloud-regions/data-regions/hipaa/

OLS Cloud Services, which may contain PHI, are assessed annually against applicable provisions within the HIPAA Privacy Rule, HIPAA Security Rule and the HITECH Breach Notification Rule.

Hébergeur de Données de Santé (HDS)

The approach taken by regulated organizations to the collection of data for purposes of clinical trial/investigations or drug/device vigilance may require the handling of such data from French data subjects. Under L.1111-8 of the French Public Health Code, as amended by Law No. 2016. Hébergeur de Données de Santé (HDS) is an ISO/IEC 27001 based approach, originally introduced by the Agence Française de la Santé Numérique, ASIP Santé (now known as the L'Agence du Numérique en Santé, ANS) which provides a framework for the handling of personal health data relating to French data subjects.

Oracle Cloud Infrastructure used in the delivery of OLS Cloud Services is independently assessed, by a third party, against HDS requirements for a Physical Infrastructure Provider and an IT Managed Services Provider. Certification is detailed on the L'Agence du Numérique en Santé (ANS) website.

Quality Management

Quality Management Systems (QMS)

To assist regulated organizations in meeting their regulatory requirements for system validation, OLS develops and maintains both products and cloud services in accordance with processes specified in the OLS quality management system (QMS). The OLS QMS details software development lifecycles (SDLCs) which define the requirements for product specification, design, formal testing, and release. In addition, the QMS encompasses OLS Cloud Services Support and Consulting Services (for provision of configuration services) where applicable.

The OLS QMS Charter forms the apex document of the QMS and establishes the quality framework designed to ensure OLS software products, cloud and consulting services are compliant with relevant GxP requirements for data integrity and system reliability applicable to the development, deployment, and support of computerized systems.

The OLS QMS is adapted from United States 21 CFR Part 820; Quality System Regulation (QSR), ISO 9001 and the United Kingdom MHRA Good Clinical Practice (GCP) Guide. Oracle policies and procedures for software development have been designed to align with the general requirements of various documents including FDA Guidance on General Principles of Software Validation, IEEE standards, ICH E6 (GCP) as well as the ISPE GAMP 5 guide. For example, Oracle has implemented elements of risk management, supplier management and validation planning into the SDLC. The QMS captures the components of the quality framework aimed to consistently provide value to regulated organizations and a superior ownership experience in service by meeting quality objectives demonstrated by, but not limited to innovation, teamwork, process improvement and compliance adherence.

The OCI Information Security Management System (ISMS) and QMS framework provides the controls for security, quality and service standards supporting applicable GxP guidelines.

OCI's ISMS (aligned with ISO/IEC 27001, 27017, 27018 and 27701) and QMS (aligned with ISO 9001) augment the processes described in the OLS QMS.

Training

Oracle conducts training of personnel involved in the delivery of Cloud Services and development of OLS Cloud Service software products.

OLS employees are required to undertake mandatory global compliance courses which include modules on:

- Corporate Compliance Policies
- Oracle's Code of Ethics and Business Conduct
- Information Protection Awareness

As well as corporate level training, OLS personnel must complete further training on the following:

- HIPAA/HITECH
- Cloud Privacy and Security awareness
- Regulations/guidance for the conduct of clinical studies and drug/device vigilance
- Role based training on applicable QMS documents

Contingent workers or contractors, dependent on their operational scope, are also required to complete OLS training.

Compliance Collateral

OLS demonstrates its ability to help regulated organizations meet their regulatory requirements, through a combination of standard assessment reports, assertion of compliance, and certifications (e.g., SOC 2, ISO 9001, ISO 27000 series, and HIPAA). Regulated organizations can rely on OCI certifications and assessment reports for in-scope cloud services to provide assurance to the effectiveness of its controls. OLS also publishes a range of materials to assist regulated organizations with their compliance obligations. Depending on the Cloud Service, the following may be available:

- Product statements (Doc ID 1470961.1) - see My Oracle Support
- Regulatory Compliance Addenda (*available for InForm Cloud Service (Doc ID 2158526.1), IRT Cloud Service (Doc ID 2256629.1) and Clinical One Cloud Services (Doc ID 2282809.1)*) - see My Oracle Support
- Product Verification Packages, PVP - see My Oracle Support or contact Your Oracle Sales representative (*available for Argus, Central Coding, Central Designer, Clinical One, CRF Submit, Data Management Workbench (DMW), Empirica Signal, IAMS, InForm suite, Safety One Intake, Study Start-up (SSU) and User Management Tool (UMT))*
- Compliance Attestations, more information available at Oracle Cloud Compliance
- Product and Service Feature Guidance - see My Oracle Support (Doc ID 111.1)

Access to My Oracle Support (MOS) requires specific login credentials.

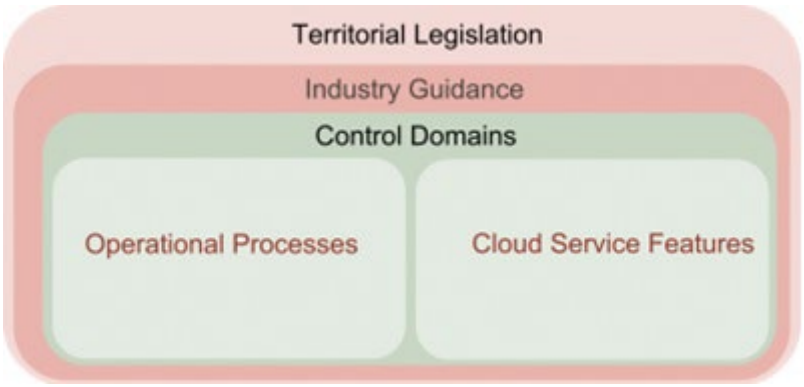
GxP Guidance Considerations

GxP guidance may be published on a country, regional, trans-regional or for a GxP specific domain. Increasing international co-operation has led to the development of globally applicable standards that may be enforceable through legislation. Within all such guidance's it is possible to distil a series of common controls which drive the security, traceability, accountability and data integrity of computerized systems used in life science operations. Controls seek to ensure electronic records are reliable and products are developed and manufactured to meet patient safety and quality standards.

Figure 2, below, highlights the compliance hierarchy leveraged during the delivery of OLS Cloud Services built on and utilizing OCI. Regulatory guidelines drive the establishment of GxP domains which result in the implementation of appropriate operational processes.

Product capabilities such as audit trails or electronic signatures are used by regulated organization end-users and may be configured by regulated organizations or OLS via consulting engagements.

Figure 2: Compliance Hierarchy



Regulated organizations leveraging OLS Cloud Services need to determine the specific GxP guidance applying to their use, and a) assess the level of vendor supplied documentation, and b) undertake regulated organizations driven validation activities to demonstrate their adherence to GxP guidelines and system specifications have been met.

The compliance domains detailed below provide a summary only and are not designed to be a comprehensive evaluation of regulatory requirements. Each domain highlights key responsibilities for each party within the cloud shared management model.

Data Integrity & Record Retention

Under GxP guidelines, data integrity can be defined as the degree to which data is complete, consistent, accurate, trustworthy and reliable[i]. GxP systems should be designed, implemented, and operated under documented procedures and controls. Such documentation should include data backup, archive/retrieval, audit trail retention, protection, and destruction procedures.

Customer: The customer will implement record retention practices assuring the integrity of their data is retained for archiving, analysis and reporting purposes. The customer will determine the record retention period for data extracted from Oracle Cloud Services and for any associated documentation associated with their use of the Cloud Service.

Oracle: Oracle Information Security Policy establishes the principles to protect, manage, and secure information assets, in accordance with business, legal, regulatory, and contractual requirements. OCI's fault tolerant infrastructure is designed with multiple layers of redundancy available for data and service resiliency, backups, and availability. OCI implements integrity protection specific to underlying systems including patch management and malicious code protection. Oracle Cloud Services backup and restore capabilities are integral to the delivery in accordance with applicable service descriptions.

Access Management

GxP guidelines require a documented process be in place to define user access and privilege levels for computer systems used in GxP regulated activity. Access and privilege should be in line with the responsibility and function of the individual, and apply appropriate controls to ensure data security, availability, confidentiality, and integrity. Access should be limited to authorized individuals, and data deletion, amendment or system configuration privileges should be restricted to system administrators. All access rights should be documented, and records maintained in accordance with the applicable GxP guideline(s).

Customer: Customers will manage and review user's role and level of access to the Cloud Service ensuring only authorized users are accessing OLS and any applicable data. Customers will assess any external identity providers they may wish to integrate with OLS Cloud Services. Please refer to Oracle product/service documentation for further details on identity federation.

Oracle: Oracle provides access management mechanisms for OLS Cloud Services to facilitate customer management of their users and associated permissions in accordance with applicable Service Descriptions. Authorization may leverage Oracle Identity and Access Management services or external federated identity providers. Administrative, technical and physical safeguards exist to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration or destruction. Access to OCI and services supporting the OLS Cloud Services are based upon the principle of least privilege, and require multi-factor authentication, a VPN connection, and a SSH connection with a user account, password and private key. OCI secure access policies and procedures are subject to independent annual audits.

For more information about Oracle's access control practices: https://www.oracle.com/corporate/security-practices/corporate/access-control.html.

Audit Trail

Under GxP guidelines, regulated activities are required to maintain appropriate records enabling the reconstruction of data collection and processing history. Accordingly, there should be a documented procedure for the maintenance of all GxP system evidence, to include appropriate reviews of audit trails.

Customer: Customers will manage record retention obligations and audit trail review according to regulatory guidance's, by exporting audit trail information from OLS Cloud Service applications.

Oracle: Oracle provides audit trail capabilities, in our OLS Cloud services, to record data entry and updates against the associated user. Date and time is recorded against a time standard. Event logs from the OLS Cloud Service including those held within the Security Incident and Event Management (SIEM) system, are protected against unauthorized access and audited at regular intervals.

Change Management

Under GxP guidelines, a documented change management process is integral to supporting the quality and integrity of cloud service operations. Change management standard operating procedures (SOPs) should be followed when upgrading applications and / or infrastructure components (for example database or operating system). Procedures should address request tracking, impact analysis, testing, security reviews and approval processes.

Customer: The customer will review product verification package material or related documents for the conduct of assessments in the evaluation environment.

Oracle: Oracle will provide upgrades to the OLS Cloud Service application and infrastructure components, periodically, in accordance with hosting and delivery policies. Upgrade pathways are developed and assessed during product development. Upgrades follow specific qualification instructions; documentation is generated for customer consumption.

Configuration Management

Under GxP guidelines, a documented configuration management process works to assure relevant parameters (such as data collection items/forms) reflects customer requirements for their intended use of the OLS Cloud Service.

Customer: The customer is responsible for defining requirements when Oracle is providing trial consulting services and undertakes the verification of any configuration files/scripts which they may prepare.

Oracle: Oracle will provide when trial consulting services are contracted, the delivery process which provides the definition and customer specifications approval. Documentation is retained for the verification of configured functionality (for example, automated query texts or workflow requirements). Oracle will provide access to suitable evaluation environments to the regulated organization. The deployment of configuration files/scripts follows necessary Oracle processes which include the use of ticketing systems.

Incident Response

GxP guidelines address the need to maintain the confidentiality, integrity and availability of data arising from regulated activities. Measures are required to enable timely and effective action for events such as the loss or unlawful destruction of regulated data to limit any further compromise of data and ensure that notification to appropriate stakeholders occurs in accordance with contractual or legal requirements.

Customer: The customer will evaluate incidents communicated by Oracle regarding their use of the OLS Cloud Service and will undertake notifications to regulatory authorities as required by law. The customer will leverage Oracle attestations, certificates, and externally published security resources to assess Oracle security incident practices. For additional information, see https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html.

Oracle: Oracle has established an Information Security Incident Reporting and Response Policy which defines requirements for monitoring, reporting, and responding to OLS Cloud Service security incidents including notification to affected customers, if applicable. Upon discovery of an incident, Oracle defines an incident response plan for rapid and effective incident investigation, response, and recovery.

Incident response plans are periodically evaluated, and external assessors perform an annual assessment of in-scope OLS Cloud Services against ISO/IEC27001 (including ISO/IEC 27018) and the applicable implementation specifications within the HIPAA Security & Privacy Rules and HITECH Breach Notification requirements.

In the event Oracle determines that a confirmed security incident involving Information processed by Oracle has taken place, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services (please refer to https://www.oracle.com/contracts/cloud-services/#data-processing).

Physical & Logical Security

GxP guidance on physical and logical security policies, procedures and controls are foundational to prevent unauthorized access, loss, damage, or changes to the Cloud Service and data. Appropriate security measures may include the use of a key, such as pass cards, passwords, biometrics, or restricted access to computer equipment and data storage areas. Security policies and procedures should be documented with the level of detail sufficient to enable periodic review and validation.

Customer: The customer is responsible for security measures restricting access to its own facilities and locations. This includes physically securing access, the transmission, and restricting the display of data to authorized personnel.

Oracle: Oracle will provide a multi-layered approach to physical and logical security controls. Physical and environmental security controls restrict access to OCI data halls within co-location facilities, its own premises, and other locations where it operates. Data in-transit encryption and data at-rest encryption is used to prevent access from unauthorized users. Oracle will also undertake penetration and vulnerability testing of its OLS Cloud Services.

Personnel Training & Education

GxP guidance require persons who participate in the conduct of a regulated activity (such as creating and updating electronic records) have the education, training, and experience to perform their assigned tasks. This typically includes having appropriate documented training plans and personnel management policies and procedures in place.

Customer: The customer will implement screening, training, and education programs to ensure personnel, agents or associated investigational site personnel have the knowledge and experience required to meet GxP guidelines including familiarity with features/functionality of the Cloud Service being used.

Oracle: Oracle will provide mandatory security & privacy awareness courses to their employees (see section on Training). Personnel with direct involvement in the development, application management, support, or configuration (via trial consulting services) of OLS Cloud Services will undertake role based training and regulatory awareness training (which encompasses applicable aspects of the United States 21 CFR Part 11 Rule and ICH E6 (GCP) Guideline). Training is driven by Oracle policies and procedures, in particular those detailed in the OLS Quality Management System.

Validation

GxP guidelines for example, ICH E6 (GCP) guideline (R2)[ii], detail the need for the validation of electronic systems for use in GxP regulated processes. While "validation" itself is variously defined within applicable GxP guidelines, it can be considered as an activity…"*to demonstrate that a system, consisting of a controlled business process which has attributes of People and Procedures, Hardware and Software, is fit for purpose and performs consistently and that changes are consistently controlled*"[iii]. Validation provides assurance that the needs of the customer are met and aims to establish accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

Validation encompasses end-to-end processes for the design, development, implementation, and use of computerized systems. Software testing (also termed verification) is a key component of an overall validation strategy. Software testing may be undertaken by a vendor for commercially available off the shelf (COTS) or custom developed software applications and Cloud Services.

Where software applications and Cloud Services require configuration to address customer requirements further evaluation should be undertaken to confirm customer requirements have been attained. Customers should leverage vendor documentation for such configuration activities according to their internal validation practices.

The installation and deployment of software used for Cloud Service delivery should be undertaken in a controlled manner using assessed installation protocols.

Customer: The customer will perform their own evaluation of the Cloud Service (and any necessary configuration of the service) to determine its suitability for their GxP regulated activity. Customers should maintain documentary evidence of such an evaluation and retain records pertaining to the specification of the Cloud Service and any approvals undertaken by the Customer.

Oracle: Oracle provides OLS Cloud Services developed under a defined software development lifecycle (SDLC). This is detailed within the OLS Quality Management System section which includes design, development, testing, implementation, verification, and release. OLS retains documentation on

development activities which may include specific customer consumable Product Validation Packages (PVPs) summarizing testing performed by Oracle during release cycles.

Deployment onto OCI follows standard protocols evaluated during development. OCI supports customer regulatory requirements with infrastructure developed and maintained in accordance with Oracle quality, security, and system management standards together with requirements detailed in external certifications.

Oracle provides customers access to assessments and user acceptance testing environments as detailed in applicable Service Descriptions.

CONCLUSION

Regulated organizations subject to GxP regulations and guidance's must be aware of their obligations within the shared management framework when utilizing OLS Cloud Services. Contract documentation, policies and practices assist customers in meeting their regulatory obligations. It also outlines customer responsibilities relating to their use of Oracle Life Sciences Cloud Services.

Oracle's established processes addresses control domains discussed in this paper (physical and logical security, personnel training and education, quality management, and access management). Oracle provides information to assist regulated organizations when evaluating Oracle security, product development and other practices and to aid in any risk-based validation activities the customer may wish to undertake.

[i] Medicines & Healthcare products Regulatory Agency (MHRA), "GxP' Data Integrity Guidance and Definitions, (March 2018), Page 9

[ii] International Council on Harmonization of Technical Requirements for Pharmaceuticals for Human Use: Integrated Addendum to ICH E6(R1): Guideline for Good Clinical Practice E6(R2)

[iii] Computerised Systems Validation in Clinical Research: A Practical Guide. Second Edition. ADCM/PSI