Oracle Tech Cloud GxP Position Paper – December, 2016

Prepared By:

Subbu Viswanathan, Head of Solutions

USDM Life Sciences

Reviewed By:

David Blewitt, VP Cloud Compliance

USDM Life Sciences

Disclaimer:

This document is intended for informational purposes only for Life Science companies who choose to use Oracle's Public Cloud for GxP use. USDM does not represent or warrant that the use of the information or recommendations contained herein will result in GxP compliance, ensure validation of GxP applications on OTC or that the recommendations contained herein will be acceptable to regulatory authorities. USDM expressly reserves the right to update or change the information and views expressed herein without notice. Moreover, USDM is under no obligation to update the information contained herein.

Limitation of Liability:

In no event shall USDM or any of its affiliates or the officers, directors, employees, members, or agents of each of them, be liable for any damages of any kind, including without limitation any special, incidental, indirect, or consequential damages, whether or not advised of the possibility of such damages, and on any theory of liability whatsoever, arising out of or in connection with the use of the information contained herein.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 STATEMENT OF INTENT

Oracle Managed Cloud Services (OMCS) delivers enterprise-grade, end-to-end managed services across every layer of the Oracle Cloud technology stack. OMCS offers Governance, Service Level Agreements, Functional and Integration Services, and Managed Security and Compliance Services.

OMCS has been delivering superior management and support of business-critical production systems and environments for over 17 years. OMCS experts leverage cloud automation tools for application provisioning, patching, upgrades, backup, and restore. Over 15,000 Oracle service professionals provide deep expertise at every layer of the Oracle stack.

Leveraging the Oracle Tech Cloud (OTC - IaaS and PaaS) OMCS helps Oracle application customers realize cloud infrastructure benefits including elastic scaling, rapid provisioning and protection from platform obsolescence. OMCS customers achieve increased productivity, reduced business risk and lower cost of ownership while maintaining a robust and secure managed environment.

1.2 EXECUTIVE SUMMARY

This paper is intended as a reference guide to those in the life science community who intend to host a validated application (validated to automate or digitize a GxP business process) on Oracle Tech Cloud (OTC). OTC provides computing resources and infrastructure (e.g. virtual machines, databases, and storage) built to customer specifications that support an end-use application (e.g. Oracle Agile or Oracle E-Business Suite) and as such OTC's services can be considered as Category 1 – Infrastructure Software as defined by GAMP5®.

This paper may be used, in conjunction with other certifications and audit reports (e.g. SAE 16 SOC1, SOC2; ISO certifications) provided by Oracle, to determine the applicability of OTC's controls to a life science customer's qualification / validation / risk framework. It provides a broad overview of the various controls contained in OTC which are designed to help a customer validate and maintain a GxP application in a validated state. It also provides a number of suggestions, based on certain assumptions; regarding controls a customer should have in place in order to use OTC to host a GxP application.

This information contained herein is based on a review of SSAE 16 SOC1 and SOC2 audit reports along with ISO certifications and interviews with Oracle's Security Compliance group personnel between September 2016 and November 2016. USDM acknowledges that controls targeted towards SSAE 16 SOC1, SOC2 or ISO certifications are not the same as GxP controls although they may share similar objectives to GxP controls. These controls are discussed in greater detail within this document and discussed in the context of FDA 21 CFR Part 11 Electronic Records; Electronic Signatures and EudraLex Volume 4 - Annex 11 Computerized Systems.

The information and recommendations provided herein are USDM's interpretation of OTC's controls and capabilities to support a GxP application. Notwithstanding, each user of an OTC hosted application should review and determine their exact requirements and determine the adequacy of OTC's controls with their own internal SOPs, policies and risk management guidelines.

1.3 PURPOSE

The purpose of this paper is to provide guidance to life science customers who intend to use OTC to host a GxP application. This paper provides a broad overview of the various controls contained in OTC which are designed to help a customer validate and maintain a GxP application in a validated state. It also provides suggestions on controls a customer should have in place in order to use OTC to host a GxP application. Notwithstanding, each user of a OTC hosted application should review and determine their exact requirements and it is still a life science customer's responsibility to ensure that the GxP application hosted on OTC is validated for intended use and to determine the adequacy of OTC's controls with their own internal SOPs, policies and risk management guidelines.

1.4 SCOPE

The information contained in this paper is based on the following regulations:

- FDA 21 CFR Part 11 Electronic Records; Electronic Signatures: Note: Only Subparts A and B, Sections 11.10 and 11.30 from this regulation are covered in this position paper. Subpart C, related to electronic signatures is not covered in this document since electronic signature capability is typically built into the end-use application. OTC does not provide electronic-signature functionality as part of their service.
- EudraLex Volume 4 - Annex 11 Computerised Systems.

This paper discusses the OTC infrastructure comprised of:

- Infrastructure software and tools (e.g. Virtual machines, database, virtualization infrastructure, storage area network),
- Networking components (e.g. firewalls, routers/switches, directory services), infrastructure hardware (filers, host machines etc.)
- Data center facilities themselves
- Quality management system that consists of processes (e.g. change management, incident management)
- Programs / tools (e.g. My Oracle Support).

1.5 USDM METHODOLOGY

In developing the recommendations and guidance contain herein, USDM reviewed:

- The audit reports, certifications and documentation listed in Appendix 2: Oracle Documentation Available For Review.
- Interviews with personnel from Oracle's Security Compliance Group and review of additional process documentation and systems that were provided during these interviews.

The following processes were also reviewed:

- Risk Based Controls for Infrastructure and Ancillary Quality Systems
- Change Management
- Configuration Management

- Incident Management / Help Desk
- Security Management
- Training Management
- Document Management
- Backup Archive and Restore
- Disaster Recovery / Business Continuity
- Physical and Environmental Controls
- Internal Audits and External Audit Support

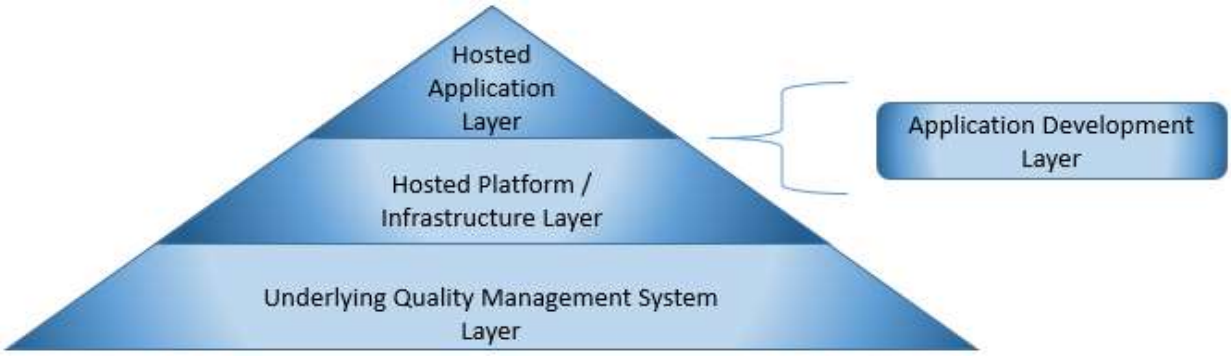
The interview process generally consisted of:

- Review of the process using process documentation / procedure / SOP / workflow or process flow diagrams.
- Review of Roles and Responsibilities (who, what, where, when)
- Review of 'hand-shakes' and interfaces between various responsible groups and personnel were discussed and reviewed.
- Review of the tools used for a particular process.
- Review of the level of controls present on the tools.
- Review of training and awareness of the process, documentation and tools by responsible personnel.

1.6 DEFINITIONS / ACRONYMS

See Appendix 1: Glossary of Terms.

2 QUALITY FRAMEWORK



Customer's typically host a GxP application (e.g. Oracle's Applications Unlimited products such as Oracle E-Business Suite or Oracle Agile PLM) on the OTC infrastructure. The application is generally developed by a software provider (like Oracle) and validated for intended use by the customer (with Oracle support). The OTC infrastructure consists of infrastructure software and tools (e.g. Virtual machines, database, virtualization infrastructure, storage area network), networking components (e.g. firewalls, routers/switches, directory services), infrastructure hardware (filers, host machines etc.) and the data center facilities themselves. Supporting the

application and the infrastructure is a quality management system which is comprised of processes (e.g. change management, incident management) and programs / tools (e.g. My Oracle Support). These different layers are discussed in sections below.

Customers can host applications on OTC in two ways:

- Customers manage the application. Oracle provides only Compute resources (e.g. virtual machines, database resources),

OR

- Oracle's Managed Cloud Services (OMCS) performs Application Management Services of the application that is hosted on OTC.

2.1 HOSTED APPLICATION LAYER

2.1.1 INITIAL VALIDATION

If OMCS is used, Oracle will install and configure the end use application per documented customer specifications and provide documented evidence that the application was installed and configured per specifications via executed installation qualification documents.

The end use application validation is ultimately the responsibility of the customer and Oracle only provides the design and installation qualification artifacts as described in the next section for the compute resources as well as the application install as described above. The customer is responsible for documenting requirements, application design, risk assessments, functional testing, and additional installation / configuration verifications of installation / configuration tasks performed by the customer as well as managing traceability.

2.1.2 MAINTENANCE OF VALIDATED STATE

Changes to the customer environment follow a documented change management process. Changes are recorded in My Oracle Support and the customer is responsible for approving all changes to their specific environment (See Section 2.4.2). Service Requests and incidents are typically recorded in My Oracle Support and the customer has access to all service requests (See Section 2.4.4). Oracle will provide documentation to the customer if significant changes are made to the environment that warrant additional documentation support or modifications to the design or installation qualification documentation provided by Oracle during the initial validation. This support will be determined via the change management process and ongoing SLAs between the customer and Oracle. Customers are responsible for functional verifications of changes made to their environment and maintaining the overall validation package for the application / environment. Oracle's underlying quality management system layer (Section 2.4) further supports the overall validated state of the customer environment.

2.2 HOSTED PLATFORM / INFRASTRUCTURE LAYER

2.2.1 CUSTOMER SPECIFIC COMPUTE RESOURCES (INFRASTRUCTURE)

2.2.1.1 Initial Qualification

OTC provides (per customer request and established SLAs) compute resources for use by the end use application. These compute resources are installed per customer requirements and the design of these components are documented by Oracle in a design document that is then provided to the customer to be included as part of the validation package for the application. Oracle will provide documented evidence of the deployed compute resources via executed installation qualifications that can be included by the customer in the validation package.

The end use application validation is ultimately the responsibility of the customer and Oracle only provides the design and installation qualification artifacts as described above for the compute resources as well as the application install. The customer is responsible for documenting requirements, application design, risk assessments, functional testing, additional installation / configuration verifications of installation / configuration tasks performed by the customer as well as managing traceability.

2.2.1.2 Maintenance of Validated State

Changes to the customer environment follow a documented change management process. Changes are typically recorded in My Oracle Support and the customer is responsible for approving all changes to their specific environment (See Section 2.4.2). Service Requests and incidents are typically recorded in My Oracle Support and the customer has access to all service requests (See Section 2.4.4). Oracle will provide documentation to the customer if significant changes are made to the environment that warrant additional documentation support or modifications to the design or installation qualification documentation provided by Oracle during the initial validation. This support will be determined via the change management process and ongoing SLAs between the customer and Oracle. Customers are responsible for functional verifications of changes made to their environment and maintaining the overall validation package for the application / environment. Oracle's underlying quality management system layer (Section 2.4) further supports the overall validated state of the customer environment.

2.2.2 CUSTOMER AGNOSTIC INFRASTRUCTURE SERVICES AND COMPONENTS

Oracle controls all of their ancillary support systems (e.g. My Oracle Support, Document Management systems, and Training Management systems) and customer agnostic infrastructure (e.g. SAN, Virtual Infrastructure) as described in Section 2.4.1. Where appropriate (e.g. My Oracle Support), customer specific configurations are tested to verify intended use and evidence for these verifications (installation and operational qualification) are provided to the

customer. These ancillary support systems and customer agnostic infrastructure services are maintained using change management process described in Section 2.4.2.

2.3 APPLICATION DEVELOPMENT LAYER

Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products. Oracle's goal is to ensure that Oracle's products, as well as the systems that leverage those products, remain as secure as possible.

Oracle Software Security Assurance is a set of industry-leading standards, technologies, and practices aimed at:

Fostering security innovations. Oracle has a long tradition of security innovations. Today this legacy continues with Oracle's market leading database security and identity management solutions.

Reducing the incidence of security weaknesses in Oracle products. Oracle Software Security Assurance key programs include Oracle's Secure Coding Standards, mandatory security training for development, the cultivation of security leaders within development groups, and the use of automated analysis and testing tools.

Reducing the impact of security weaknesses in released products on customers. Oracle has adopted transparent security vulnerability disclosure and remediation policies. The company is committed to treating ALL customers equally, and delivering the best possible security patching experience through the Critical Patch Update and Security Alert programs.

2.4 UNDERLYING QUALITY MANAGEMENT SYSTEM LAYER

2.4.1 RISK BASED CONTROLS FOR INFRASTRUCTURE AND ANCILLARY QUALITY SYSTEMS

All support infrastructure (e.g. SAN, Database infrastructure, etc.) and ancillary support systems (e.g. My Oracle Support (MOS), Backup system) are maintained in a state of control. This is achieved via internal SLAs with system owners who own the various systems as well as confirmation of process and controls via ISO 20000 and SOC 2 audits. These systems are also maintained using change management processes described in Section 2.4.2. Additionally, the SOC1 audit reported that Oracle manages the OTC platform following a Risk management methodology. Where appropriate (e.g. My Oracle Support), customer specific configurations are tested to verify intended use and evidence for these verifications (installation and operational qualification) are provided to the customer.

2.4.2 CHANGE MANAGEMENT

Oracle has established a documented change management and change control process for application and infrastructure services specific to each customer as well as ancillary systems and customer agnostic infrastructure that enable Oracle to provide the hosting services. Oracle's change management program specifically includes customer involvement (via request and approvals using My Oracle Support) for all changes that affect the

customer's environment. Oracle will provide documentation to the customer if significant changes are made to the environment that warrant additional documentation support or modifications to the design or installation qualification documentation provided by Oracle to the customer during the initial validation. Additionally, for systems supported by OMCS, Oracle may use customer change ticketing systems (based on applicable SLAs).

Change management process broadly covers:

- Change requests by authorized personnel.
- Change request tracking to completion.
- Change approval.
- Impact assessments for each change.
- Roll back and contingency processes.
- Change promotion through various environments (e.g. test, pre-production, production environments).

My Oracle Support tickets are maintained per Oracle's standard record retention policies. Customers can request to extend these record retention policies or request Oracle to utilize the customer's ticketing systems as part of the service.

2.4.3 CONFIGURATION MANAGEMENT

Oracle manages their compute assets and customer agnostic infrastructure and systems using a configuration and asset management tool that stores information about each asset as well as its current configuration state. Customer specific infrastructure are managed using the change management process described in Section 2.4.2. It is the customer's responsibility to maintain configuration records and specifications for their environment. Oracle will provide necessary documentation to the customer depending on the change and established SLAs between the customer and Oracle. It is up to the customer to maintain these records along with the validation package for their application.

2.4.4 INCIDENT MANAGEMENT / HELP DESK

Oracle has a documented incident and service request tracking process for application and infrastructure service issues or service requests specific to each customer. Oracle also has an internal incident management system for ancillary systems and customer agnostic infrastructure services that enable Oracle to manage and maintain their systems. Additionally, internal monitoring tools monitor critical parameters of the compute environment in order to escalate issues and monitor the health of the overall environment. Oracle's incident management program specifically includes customer involvement (using My Oracle Support) for submitting, reviewing and approving service request tickets and incident tickets. Additionally, for systems supported by OMCS, Oracle may use customer service / help desk ticketing systems (based on applicable SLAs). My Oracle Support tickets are maintained per Oracle's standard record retention policies. Customers can request to extend these record retention policies or request Oracle to utilize the customer's ticketing systems as part of the service.

2.4.5 SECURITY MANAGEMENT

Oracle has a multi-dimensional strategy for managing security of their data center as well as customer data and systems that are controlled and managed by Oracle. It is assumed that the security of the customer's data is not Oracle's responsibility alone but also the responsibility of the customer. The customer has to ensure adequate security procedures as well as systems are in place to ensure system security. Oracle's security management covers the following:

- Executive oversight of the security organization.
- Detailed training program to ensure security policies and practices are adhered to across the organization.
- Maintenance of compute assets using an asset management system with clear roles, authority and accountability for each asset.
- Identity and access management systems that provide relevant access to qualified personnel while restricting non-named user accounts (e.g. root accounts or service accounts). These systems are linked to HR systems to ensure terminated personnel no longer have access to systems.
- Security Information and Event Management systems that monitor security incidents and report them for timely resolution.
- Intrusion Detection Systems that report intrusions for timely resolution.
- Periodic vulnerability assessments to ensure various hardware and software layers are adequately hardened against vulnerabilities.
- Periodic review of access privileges to ensure only appropriate personnel have the access to systems.
- Oracle Security and Compliance team performs Quarterly Vulnerability Scanning of the customer's environment as part of the GxP Service Package. The results of the scans are reviewed with the customer in a Quarterly meeting.
- As part of the GxP Service Package the customer is also entitled to a yearly Penetration Test.
- All compute resources are set to UTC (Universal Time Clock) and are synchronized using Network Time Protocol (NTP) with a central time server clock.
- Oracle enforces strong password policies on all infrastructure and application software components (minimum length, complexity, history, expiry, lock out etc.).
- Where appropriate IP black/white listing and other secure access tunnels (e.g. VPN tunneling) are provided to customers to restrict access to their compute resources and data.
- Where appropriate data encryption (both at rest and in motion) can be provided to customers based on applicable SLAs.

2.4.6 TRAINING MANAGEMENT

Oracle ensures all technical and support personnel managing the Infrastructure as well as customer applications are adequately trained for their

job function. Training records are managed via a corporate Training Management System. Personnel training is the responsibility of individual team managers. Personnel training includes training on job function as well as training on procedures and policies and relevant industry level training (where applicable). Training records and personnel's training statuses are reviewed periodically by the internal audit team. Where required, OMCS personnel can be trained on customer specific training procedures and these are based on applicable SLAs. These customer training records will be managed by the customer's training management systems.

2.4.7 Document Management

Oracle utilizes a consistent document management process and has a Document Management System that maintains all relevant procedures and documentation. Oracle documentation go through formal review, approval and update processes and are accessible by relevant personnel. The Document Management System also prevents unauthorized edits / deletions. Customer systems' validation and qualification deliverables are provided by Oracle to the customer and it is the customer's responsibility to maintain these documents as part of their Document Management System.

2.4.8 Backup / Archive / Restore

Oracle provides comprehensive backup services to customer's data, database and the virtual machines themselves. Backup frequencies are determined based on SLAs with end customers but typically include daily incremental and weekly full backups. Restores of backed up data are tested weekly. These restore tests include data integrity checks of the data restored. Restores are tested at varying levels of granularity (e.g. specific files vs entire virtual server or specific records vs entire databases). Backups typically occur from Disc to Disc to Tape (Tapes are stored off site at Iron Mountain). Data retention of the backups are configured per customer's specific needs and SLA stipulations. Restore requests from customers are restricted to few personnel and these requests are documented in service request tickets (described in Section 2.4.4).

2.4.9 Disaster Recovery / Business Continuity

Oracle provides a comprehensive disaster recovery solution to customer's application, as well as structured data (database), unstructured data (files) virtual machines. Oracle provides typically an annual Disaster Recovery test where they work with the customers to recover the customer's systems in the disaster recovery data center. Results of these tests are provided to the customer to include with any qualification / validation documents.

2.4.10 Physical and Environmental Controls

Oracle's data centers demonstrate physical and environmental controls that ensure the protection of the physical hardware within the data center. Oracle provides comprehensive physical security to prevent unauthorized physical access. This includes physical security, physical access controls, security personnel and surveillance. Additionally, environmental controls are in place (e.g. fire suppression, emergency power) to further safeguard the physical assets. Disaster Recovery programs are in place in case of a catastrophic data center failure as described in Section 2.4.9.

2.4.11 INTERNAL AUDITS AND EXTERNAL AUDIT SUPPORT

Oracle has an internal quality audit group that periodically reviews all service areas to ensure conformance to process. Non-conformances are tracked using an audit management tool and tracked until resolution. The internal audit team covers all aspects of the quality system described in this document.

Oracle also entertains external audits from Third Party Auditors (e.g. SOC1, SOC2 audits, ISO certifications).

Additionally, Oracle entertains quarterly reviews with their customers (where service requests and incidents relevant to the customer's systems and services are reviewed with the customer) and annual audits with their customers where a formal audit visit by the customer is entertained by Oracle on the customer's systems and services being supported by Oracle.

3 REGULATORY FRAMEWORK

Assessment of Compliance with US FDA, 21 CFR Part 11 and Eudralex, Volume 4: Annex 11

3.1 QUALITY SYSTEMS

3.1.1 RISK MANAGEMENT

EU Annex 11 (1):

Risk management should be applied throughout the lifecycle of the computerised 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 computerised system.

OTC Controls:

Oracle has a process for supporting the qualification/validation of their customer specific infrastructure and application (described in Sections 2.1.1, 2.2.1). Additionally, Oracle applies a risk management framework for the OTC infrastructure and Oracle manages the infrastructure and ancillary systems using the controls as described in 2.4.1.

Customer Controls:

The customer is responsible for ensuring that the end-use application and Oracle's hosing capabilities are appropriately assessed for risk and are validated/qualified commensurate with that risk following their own internal risk based validation / qualification processes.

3.1.2 SUPPLIERS AND SERVICE PROVIDERS QUALIFICATION

EU Annex 11 (3):

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 computerised 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. IT-departments should be considered analogous.

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.

3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.

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.

OTC Controls:

For customers utilizing OTC, Oracle would be a third party to the customer (since they support and maintain services and systems for the customer). Formal agreements are set up between Oracle and the customer clearly delineating roles and responsibilities.

Customer Controls:

The customer is responsible for having processes in place to evaluate and assess third parties like OTC and to determine the third parties' adequacy to the customers quality and regulatory requirements.

3.1.3 Change Control / Configuration Management

EU Annex 11 (10):

Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.

OTC Controls:

Oracle utilizes the My Oracle Support platform to manage change to a customer's specific environment. All changes are formally assessed and resolved as described in Section 2.4.2. Configuration management of the customer environment is mainly the responsibility of the customer. Oracle provides configuration information using the My Oracle Support platform as well as provides documentation associated with changes made to the configuration, but it is the customer's responsibility to manage the configuration details as part of their validation documentation. Changes to customer agnostic infrastructure is handled via internal Oracle change management processes as described in Section 2.4.2 and the configuration of these customer agnostic infrastructure is managed and maintained as described in Section 2.4.3

Customer Controls:

The customer is responsible for requesting as well as approving all changes to their environment. The customer is responsible for ensuring a change control and configuration management process is present as part of their overall quality system which will also be applicable to the system they deployed with OTC.

3.1.4 PERIODIC REVIEW

EU Annex 11 (11):

Computerised 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

OTC Controls:

Oracle quality organization conducts periodic internal audits to ensure that established processes are being followed across the organization. Oracle also provides a dedicated Service Delivery Manager that conducts quarterly reviews with the customer on customer specific metrics and controls as well as entertains an annual audit from each customer. See Section 2.4.11 for additional details on the internal and external audit process. Additionally Oracle adheres to change management and configuration management controls described in Sections 2.4.2 and 2.4.3. Oracle systems are also monitored on an ongoing basis as described in Section 2.4.4.

Customer Controls:

The customer is responsible for ensuring that a periodic review process is in place as required by Annex 11 and is responsible to ensure that the computerized system deployed on OTC is maintained per their internal change management process, issues and incidents are managed via a non-conformance and CAPA process.

3.1.5 INCIDENT MANAGEMENT

EU Annex 11 (13):

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

OTC Controls:

Oracle utilizes the My Oracle Support platform to manage incidents and issues with their service. Customers, Oracle personnel as well as monitoring systems can report incidents in this system. Incidents are then managed as described in Section 2.4.4

Customer Controls:

The customer is responsible for ensuring that processes are in place to raise and report issues to Oracle. The customer should also have processes for reporting non-conformances and deviations as well as a CAPA process.

3.1.6 BUSINESS CONTINUITY

EU Annex 11 (16):

For the availability of computerised 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.

OTC Controls:

Oracle can provide robust disaster recovery capabilities for the customer applications deployed on OTC. The Recovery Point Objectives and Recovery Time Objectives are agreed upon using SLAs with the customer. Oracle will at a minimum test the disaster recovery capability of the application once annually and provide documentation to the customer for the results of the test.

See Section 2.4.9 for additional details.

Customer Controls:

The customer is responsible for ensuring that processes are in place for a comprehensive disaster recovery and business continuity program, that includes frequent tests.

3.2 ELECTRONIC RECORDS: CONTROLS FOR CLOSED SYSTEMS

21 CFR Part 11 Subpart B 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:

3.2.1 VALIDATION

21 CFR Part 11 Subpart B 11.10 (a):

Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

EU Annex 11 (4):

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.

4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.

4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available.

For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.

4.4 User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.

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.

4.6 For the validation of bespoke or customised computerised 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.

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.

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.

OTC Controls:

Oracle can support the overall validation effort of systems being hosted on OTC but cannot guarantee the validation status of the GxP system being hosted on OTC. If Oracle manages the application (using OMCS), Oracle will also provide system design documentation as well as executed installation qualification protocols that demonstrate that the system (and its infrastructure components like database, virtual machines) are installed per approved specifications. Oracle can provide technical support to ensure that alterations to data and records can be audit trailed and alterations are clearly discernable, however the ultimate responsibility for ensuring that the system hosted on OTC is designed in a manner that ensures Part 11 or Annex 11 compliance is the customer's.

Oracle will support change management and configuration management as described in Section 2.4.2 and 2.4.3.

Oracle also maintains and manages their compute assets as described in 2.4.5 as well as controls their customer agnostic systems and infrastructure as described in 2.4.1.

Customer Controls:

Oracle customers are responsible to ensure that the GxP systems hosted on OTC are validated for intended use and meet the requirements of 21 CFR Part 11 and EU Annex 11. Customers should follow written and approved procedures to validate electronic record keeping systems used in GxP operations. The system should be designed to ensure controls like date/time stamps, system generated audit trails, digital signatures of records as appropriate. Customers should maintain a GxP system inventory as well as a validation process that includes requirements, risk assessments, design, verifications and traceability from requirements and design to verifications. Customers should also have change management procedures in place to maintain the overall validated state of the GxP system.

3.2.2 COPIES OF RECORDS

21 CFR Part 11 Subpart B 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.

EU Annex 11 (8):

8.1 It should be possible to obtain clear printed copies of electronically stored data.

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.

OTC Controls:

Oracle can provide technical support in the form of database, data management and reporting solutions to meet the requirements stipulated above. i.e. Oracle can provide tools for creating complete and accurate copies of data generated by the GxP systems hosted on OTC (e.g. database backups, Oracle dataguard) as well as provide reporting infrastructure (e.g. Oracle's Business Intelligence and reporting platforms) to further ensure that the GxP records are human readable. However, the design of the GxP system to support such requirements must be driven by the customer and the validation of these requirements are also the customer's responsibility. Oracle will provide the technical expertise and support to help design such solutions.

Oracle has robust data management and data backup (See Section 2.4.8) processes to satisfy such requirements.

Any data corruption issue encountered by OTC will be escalated and communicated with customers based on established SLAs.

Customer Controls:

Oracle customers are responsible to ensure that the GxP systems hosted on OTC are designed to provide complete, accurate and human readable copies of GxP data (including audit trails). These requirements also have to be validated by the customer to ensure that the requirements are adequately met by the designed system hosted on OTC.

3.2.3 PROTECTION OF RECORDS

21 CFR Part 11 Subpart B 11.10 (c):

Protection of records to enable their accurate and ready retrieval throughout the records retention period.

EU Annex 11 (7):

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.

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.

EU Annex 11 (17):

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.

OTC Controls:

Oracle can provide technical support in the form of database, data management, data security, data encryption and data backup, archival solutions to meet the requirements stipulated above. i.e. Oracle can provide tools for securing, backing up and archiving GxP data. However, the design of the GxP system to support such requirements must be driven by the customer and the validation of these requirements are also the customer's responsibility. Oracle will provide the technical expertise and support to help design such solutions as well as support the testing of these requirements.

Oracle has robust data backup (See Section 2.4.8) processes to ensure data is appropriately backed up as well as recoverable with data integrity checks.

Any data corruption issue encountered by OTC will be escalated and communicated with customers based on established SLAs.

Physical and Logical security for the GxP data is discussed in Sections 2.4.5 and 2.4.10, however the overall security design of the application is the responsibility of the customer.

Customer Controls:

Oracle customers are responsible to ensure that the GxP systems hosted on OTC are designed to secure stored data, backup the data as well data archival. Oracle can provide technical support to ensure that these requirements can be met via design however the customer is responsible to ensure the requirements and design encapsulate the requirements related to data backup, archival and restoration. These requirements also have to be validated by the customer to ensure that the requirements are adequately met by the designed system hosted on OTC.

3.2.4 SECURITY

21 CFR Part 11 Subpart B 11.10 (d):

Limiting system access to authorized individuals.

EU Annex 11 (12):

12.1 Physical and/or logical controls should be in place to restrict access to computerized system to authorised persons. Suitable methods of preventing unauthorised 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.

12.2 The extent of security controls depends on the criticality of the computerised system.

12.3 Creation, change, and cancellation of access authorisations should be recorded.

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.

OTC Controls:

Oracle has extensive security processes to prevent unauthorized access to Oracle's data center as well as customer data (This is described in Sections 2.4.5 and 2.4.10). However, the customer is responsible for ensuring that the security related to the system and services being hosted on OTC is appropriately managed to prevent unauthorized access. i.e. Oracle does not govern who has access to the applications from the customer perspective. This administration, permissions and management has to be controlled by the customer.

Customer Controls:

Oracle customers are responsible to ensure processes are in place for managing the security of the GxP systems hosted on OTC. These processes should include privileges management, identity and access management, password management, revoking of rights, IP address white listing / black listing, inactivity timeouts, unauthorized access lockouts etc. Oracle can provide technical guidance to ensure that the application is appropriately hardened from a security perspective, however it is the customer's

responsibility to ensure that the security management of the application is adequate. These security management requirements need to be validated by the customer to ensure that these requirements are adequately met by the system design.

3.2.5 AUDIT TRAIL

21 CFR Part 11 Subpart B 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.

EU Annex 11 (9):

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.

EU Annex 11 (12.3):

12.3 Creation, change, and cancellation of access authorisations should be recorded.

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.

OTC Controls:

Oracle has extensive security processes to prevent unauthorized access to Oracle's data center as well as customer data (This is described in Sections 2.4.5 and 2.4.10). However, the customer is responsible for ensuring that the systems being hosted on OTC are designed to have detailed audit trails that track creation, modification and deletion of GxP records. Oracle can provide technical assistance to ensure that the system is designed to achieve such audit trail requirements however it is the customer's responsibility to ensure that application design meets such audit trail requirements. Oracle administrators (e.g. Storage administrators, Database administrators) though may have access to back end audit trail records will typically be contractually bound (via SLAs) to ensure that they do not alter customer data (including audit trail records).

Customer Controls:

Oracle customers are responsible to ensure that the GxP systems hosted on OTC are designed to meet the audit trail requirements stipulated in 21 CFR Part 11 and Annex 11. The ability to have human readable audit trail that unambiguously details who created, altered, deleted what record, when and what was the change (values before and after the change). This audit trail

must be unalterable and system generated. These audit trail requirements need to be validated by the customer to ensure that these requirements are adequately met by the system design. It is the customer's responsibility to identify what records within the system are GxP records and thus require audit trails.

3.2.6 Operational System and Accuracy Checks

21 CFR Part 11 Subpart B 11.10 (f):

Use of operational system checks to enforce permitted sequencing of steps and events as appropriate.

EU Annex 11 (6):

For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be 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.

OTC Controls:

OTC can host a GxP application that has these operational checks and data validation checks. This requirement is typically fulfilled at the application design layer and is not applicable to the infrastructure provided by OTC.

Customer Controls:

Oracle customers are responsible to ensure that the GxP systems hosted on OTC are designed to meet these requirements. The operational checks are typically part of the system design and these checks need to be validated to ensure that they work as intended in the requirements.

3.2.7 Authority Checks

21 CFR Part 11 Subpart B 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.

EU Annex 11 (15):

When a computerised 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.

OTC Controls:

OTC can host a GxP application and can ensure that security credentials that provide access to the system are appropriately implemented across the technology stack. Oracle has extensive security processes to prevent

unauthorized access to Oracle's data center as well as customer data (This is described in Sections 2.4.5 and 2.4.10). However, the customer is responsible for ensuring that the security related to the system and services being hosted on OTC is appropriately managed to prevent unauthorized access. i.e. Oracle does not govern who has access to the applications from the customer perspective. This administration, permissions and management has to be controlled by the customer. Oracle also does not provide e-signature solutions at the OTC platform level. These solutions are part of the design of the GxP system and therefore are the responsibility of the customer.

Customer Controls:

Oracle customers are responsible to ensure that the GxP systems hosted on OTC are designed to meet these security and authority check requirements. Electronic signatures are also implemented at the application layer and are typically part of the system design. Oracle customers are responsible to ensure processes are in place for managing the security of the GxP systems hosted on OTC. These processes should include privileges management, identity and access management, password management, revoking of rights, IP address white listing / black listing, inactivity timeouts, unauthorized access lockouts etc. Oracle can provide technical guidance to ensure that the application is appropriately hardened from a security perspective, however it is the customer's responsibility to ensure that the security management of the application is adequate. These requirements need to be validated to ensure that they work as intended in the requirements by the customer.

3.2.8 Device / External Systems Checks

21 CFR Part 11 Subpart B 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

EU Annex 11 (5):

Computerised 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.

OTC Controls:

OTC can provide technical support to ensure this requirement can be met by the eventual design of the GxP application. These could include device checks, IP white listing / black listing and other technical controls. However, the need for device checks are to be determined by the customer and should be built into the requirements and design of the GxP application that will be hosted on OTC. Oracle can provide the necessary technical controls to ensure no external entity can access the customer's data (discussed in Sections 2.4.5 and 2.4.10).

Customer Controls:

Oracle customers are responsible to ensure that the GxP systems hosted on OTC are designed to meet these device check requirements. These

requirements need to be validated to ensure that they work as intended in the requirements by the customer.

3.2.9 Qualification of Individuals

21 CFR Part 11 Subpart B 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.

EU Annex 11 (2):

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.

OTC Controls:

OTC and OMCS have strong training management program that can adequately support this requirement. This is described in Section 2.4.6.

Customer Controls:

Oracle customers are responsible to ensure that all users and administrators of the GxP systems hosted on OTC are adequately trained in the use, maintenance and administration of the system (per their defined job function) and are responsible to maintain training records for these users and administrators.

3.2.10 Electronic Signature Accountability

21 CFR Part 11 Subpart B 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.

EU Annex 11 (14):

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.

OTC Controls:

OTC does not generate electronic records or electronic signatures. This is fundamentally a part of the GxP application design and is the responsibility of the customer.

Customer Controls:

Oracle customers are responsible for implementing controls for the use of electronic signatures (assuming the GxP application hosted by OTC is designed to utilize electronic signatures). Oracle customers are responsible for ensuring that all personnel understand and area aware of the equivalency of the electronic signature to their hand-written signatures.

3.2.11 System Documentation

21 CFR Part 11 Subpart B 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.

11.10 (k)(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation

OTC Controls:

OTC has a robust documentation management program as described in Section 2.4.7. Additional system documentation (e.g. Design documents, Installation Qualifications) are turned over to the customer to manage as part of their document management program.

OTC has a documented change management and configuration management program to manage their assets. This is described in Section 2.4.2 and 2.4.3. The customers are ultimately responsible to manage the overall configuration and change management of their end use application.

Customer Controls:

Oracle customers are responsible to manage system validation documentation as well as operations and maintenance procedures.

The customer is also responsible for requesting as well as approving all changes to their environment. The customer is responsible for ensuring a change control and configuration management process is present as part of their overall quality system which will also be applicable to the system they deployed with OTC.

3.3 Electronic Records: Controls for Open Systems

21 CFR Part 11 Subpart B 11.30:

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

OTC Controls:

OTC can host a GxP application and can ensure that security credentials that provide access to the system are appropriately implemented across the technology stack. Oracle has extensive security processes to prevent unauthorized access to Oracle's data center as well as to protect the confidentiality of customer data (This is described in Sections 2.4.5 and 2.4.10). OTC can also provide secure access tunnels to customer data (e.g. SSL, VPN), IP black listing / white listing or provide data encryption capabilities as part of established SLAs with the customer. However, the customer is responsible for ensuring that the overall design of the system (which may include interfaces with customer's on premise systems) meets the requirement of this regulation. Furthermore, Oracle does not govern who has access to the applications from the customer perspective. This administration, permissions and management has to be controlled by the customer. Oracle also does not provide e-signature solutions at the OTC platform level. These solutions are part of the design of the GxP system and therefore are the responsibility of the customer

Customer Controls:

The customer is responsible for ensuring appropriate controls and system design is in place to meet this regulation. It is up to the customer to require encryption or design their systems for encryption or IP white listing or require secure access tunnels to their data from Oracle. Oracle serves as the technology partner for customers and will assist customers to ensure system design meets customer's requirements per established SLAs.

4 Appendices

4.1 Appendix 1: Glossary of Terms

S.N	Acronym	Definition
1.	AMS	Application Management Services
2.	cGMP	Current Good Manufacturing Practices
3.	CRM	Customer Relationship Management
4.	DB	Database

S.N	ACRONYM	DEFINITION
5.	FDA	Food and Drug Administration
6.	HIPAA	Health Insurance Portability and Accountability Act of 1996
7.	IaaS	Infrastructure as a Service
8.	IDS	Intrusion Detection System
9.	IEC	International Electrotechnical Commission
10.	ISO	International Organization for Standards
11.	IT	Information Technology
12.	ITAS	IT Automation Suite
13.	MOS	My Oracle Support
14.	NDA	Non-Disclosure Agreement
15.	NTP	Network Time Protocol
16.	OEM	Oracle Enterprise Manager
17.	OMCS	Oracle Managed Cloud Services
18.	OTC	Oracle Tech Cloud
19.	PaaS	Platform as a Service
20.	RFC	Request for Change
21.	RPO	Recovery Point Objectives
22.	RTO	Recovery Time Objectives
23.	SAN	Storage Area Network
24.	SDM	Service Delivery Manager
25.	SIEM	Security Information and Event System
26.	SLA	Service Level Agreement
27.	SOC	Service Organization Controls
28.	SOP	Standard Operating Procedures
29.	SR	Service Request

S.N	ACRONYM	DEFINITION
30.	USDM	US Data Management, LLC (www.usdm.com)
31.	UTC	Universal Time Clock
32.	VPN	Virtual Private Network

4.1 APPENDIX 2: ORACLE DOCUMENTATION AVAILABLE FOR REVIEW

- Oracle Compute Cloud Service Penetration Test Documentation (January 2016)
- SSAE 16: SOC 1 Type 2 Report (December 2015)
- SSAE 16: SOC 2 Type 2 Report (December 2015)
- Oracle Cloud Hosting and Delivery Policies (July 2016)
- Oracle Cloud Security Practices for Platform and Infrastructure as a Service (PaaS/IaaS) Cloud Services (July 2016)
- Oracle PaaS and IaaS Public Cloud Services Pillar Document (July 2016)
- Oracle – Validation Support Schedule (November 2016)
- ISO/IEC 20000-1:2011 (IT Service Management System) Certificate

4.2 APPENDIX 3: CITATIONS AND REFERENCES

- U.S. Food and Drug Administration, Code of Federal Regulations, Title 21 Part 11, Electronic Records; Electronic Signatures.
- U.S. Food and Drug Administration, Guidance for Industry - Part 11, Electronic Records; Electronic Signatures - Scope and Application.
- ISPE, GAMP 5 - A Risk-Based Approach to Compliant GxP computerized systems, 2008.
- ISPE, GAMP Good Practice Guide: IT Infrastructure Control and Compliance
- EudraLex The Rules Governing Medicinal Products in the European Union - Volume 4 - Good Manufacturing Practice - Medicinal Products for Human and Veterinary Use- Annex 11: Computerised Systems