Applications Management for Oracle on Any Cloud

Service Guide

April 2024

Applications Management for Oracle on Any Cloud

Table of Contents

Applications Management for Oracle on Any Cloud

Service Guide

Application Management for Oracle on Any Cloud provides Oracle Applications Management services (Services) as described in this Service Guide at Kyndryl supported 3rd party Infrastructure as a Service (IaaS) availability domain(s)/zone(s). Client can run and manage enterprise business applications from such IaaS environments and Kyndryl will arrange for the provisioning and will manage such IaaS environments on behalf of the Client to the level of support services that the Client orders. Client will need to work with Kyndryl to deploy software and applications within the IaaS account.

Upon acceptance of the Order and Pricing Schedule (Schedule), Kyndryl will enable the ordered Services. Additional terms in a Schedule may modify this Service Guide.

Kyndryl may revise this Service Guide, including rules, policies and guidelines for use of the Services, at any time. The most recent version of the Service Guide including all updates is available at the following URL: app-mgmt-oracle-on-cloud-service-guide.pdf (kyndryl.com) . The latest dated Service Guide will prevail over an earlier version, except as may be expressly specified otherwise. If, however, a revision has a materially adverse impact on Client, Client can notify Kyndryl of the impact within 30 days of the notice of the change. If Kyndryl does not remedy the specific impacted activity within 30 days after receipt of notice from Client, Client may terminate the affected Service Component by providing Kyndryl 30 days' notice. Materially adverse impacts do not include changes required by governmental authority or assessment of or changes to additional charges such as surcharges or taxes.

Client is responsible to comply with the policies and guidelines described in this Service Guide.

SD-1. Kyndryl Portal

Client is provided with access to a portal via user id and password. Client can submit service and change requests to Kyndryl-managed Service Components and get summarized views of Service Requests, Incidents and Change Requests.

SD-2. Service Infrastructure

SD-2.1. Service Location

Kyndryl provides Services at the agreed upon IaaS availability domain(s)/zone(s). Kyndryl will deploy management infrastructure at additional sites as needed.

SD-2.2. IaaS Infrastructure

Client may choose between using Kyndryl's Public Cloud Resell Program or contract directly with the Public Cloud IaaS Infrastructure vendor. In the latter case, Client agrees to contract with one of the Kyndryl approved vendors of public cloud IaaS infrastructures to host the Services managed by Kyndryl. Client is responsible for all costs associated with IaaS and other Services directly consumed from the cloud provider.

If not using the Kyndryl's Public Cloud Resell Program, prior to starting the Service, Kyndryl will request Client to create an IaaS Admin account with one of the approved Cloud IaaS Providers. Client will provide to Kyndryl administrator credentials on the account that are capable of ordering IaaS services as needed. Client gives Kyndryl explicit approval to deploy resources as per the agreed solution to build out Client environment. Client will directly incur charges for any resources that Kyndryl deploys. Unless using Kyndryl's Public Cloud Resell Program, Client is responsible to pay for the resources directly to IaaS vendors as needed.

When the Client chooses to use Kyndryl's Public Cloud Resell Program, Client agrees to have Kyndryl perform IaaS management tasks on behalf of the Client to the level of support services that the Client orders. Such support services include provisioning, decommissioning, enabling, disabling, scaling, or performing any other tasks required to manage the IaaS and its components to the level of support services that the Client orders.

Kyndryl will provision the infrastructure, software and services for the service account to support the Services ordered by the Client in the specified availability domain(s)/zone(s). Kyndryl will:

- Provide project planning and coordination to design and provide the required infrastructure and application architecture
- Install, configure and test infrastructure, software, and services in the service account.
- Apply Kyndryl security policy

For each managed environment, based upon Client selections in the Order Document or change authorization, Kyndryl will provide:

- Monitoring the virtual machine or bare metal server availability including operating system up/down status and resource utilization,
- Management of the operating system process and logs files including response to operating system Incidents, and
- Application of operating system security and update patches according to agreed schedule and maintenance window, and as needed for critical updates.

SD-2.2.1. Maintenance

Maintenance of the Client IaaS from the OS and above is performed during agreed scheduled maintenance windows or on an as needed basis. Scheduled maintenance includes system upgrades, enhancements or routine maintenance which is announced either through the Portal or through email notification by the Delivery Partner Executive (DPE) at least two days in advance. Maintenance determined by Kyndryl to be an emergency will have notice announced through the Portal.

SD-2.3. Support for Managed Infrastructure, Equipment and Software

When Client contracts directly with the IaaS vendor, Client will need to notify Kyndryl within 15 calendar days after notification from a IaaS vendor that the maintenance of any managed equipment or software is no longer supported by its manufacturer or vendor, or that repair parts and/or patches or upgrades cannot be reasonably obtained for the equipment or software, or that another reasonably satisfactory maintenance provider is not available to maintain the equipment or software ("Support Discontinuance"). Kyndryl will inform Client if the Service will be impaired by the Support Discontinuance and advise Client of alternatives to the continued use of the affected equipment or software. If Client does not authorize Kyndryl to replace such equipment or software after notice of Support Discontinuance or otherwise make reasonable alternative arrangements within 30 calendar days following Kyndryl's notice, Kyndryl shall not be liable for failure to meet applicable service level agreements arising from the failure of equipment or software subject to the Support Discontinuance.

Client will use supported versions of Client software or will purchase extended support from the applicable vendor. Should Client cease making maintenance payments or fail to purchase extended support from the applicable vendor, thereby resulting in use of unsupported versions of Client software ("Unsupported Versions"), then (a) all necessary patches, fixes, and upgrades will be performed by Kyndryl on a time and materials basis and billed to the Client; (b) any issues under the SLA that were caused by any Unsupported Version will be excluded from the calculation of Availability; and (c) additionally, to the extent that security patches are no longer made available for any Unsupported Versions, Kyndryl reserves the right to take any necessary action which could include withdrawal of services to protect Kyndryl's network from associated vulnerabilities.

Kyndryl may provide update/migration custom services with respect to Support Discontinuance or Unsupported Versions for an additional charge to Client.

SD-3. Security

Kyndryl manages the Infrastructure under policies and procedures that are designed to provide logical/IT security. Kyndryl provides security for the Client's virtual private cloud (VPC)/virtual cloud network (VCN) included in scope.

SD-3.1. Security Services - Included

Pricing for Services are included in Client's charges. Services not listed can be provided under a separate Scope of Work for additional charges. Please refer to A-1 Security Roles & Responsibilities for additional security roles and responsibilities.

Service Feature	Included	Optional - Custom	Description
Cloud Based Network Access Control	X		Cloud native inbound and outbound filtering using security groups and network access lists. (Kyndryl will not monitor logs in the Client environment; it will be an optional service.)
Anti-Virus Protection / Endpoint Detection and Response	X		Install, configure, monitor and respond to events, for all systems running on supported operating systems.
Security Information and Event Management (SIEM)	X		SIEM is included for components in Kyndryl's management infrastructure (service account) used to deliver and manage Client solutions.
Vulnerability Scanning	X		Vulnerability scanning of Client's Kyndryl managed firewalls (excluding cloud native), all systems at the VM and OS levels, and all databases and applications built manually. PaaS and SaaS components are not included.
Data Encryption	X		Encryption of Client data at rest is enabled if encryption is provided by the IaaS.
Host Intrusion Prevention (HIPS) System	X		Kyndryl will implement and manage a Host-based Intrusion Prevention System according to Kyndryl security controls and best practices for all internet-facing virtual machines.

SD-3.2. Security Services

SD-3.2.1. Cloud Based Network Access Control

Kyndryl provisions and manages IaaS security services to support Client's policies and comply with Kyndryl security standards. During implementation, Kyndryl creates initial inbound and outbound Access Control Lists to restrict all unnecessary and unauthorized access to environments, and tests with networking components. Client requests for updates to policies are made through the change process.

SD-3.2.2. Anti-Virus Software / Endpoint Detection and Response

Endpoint detection software is installed, configured and managed on all Kyndryl managed virtual servers running on supported operating systems. Monitor and response to events generated by EDR solution is part of the services included. EDR solution is configured to meet Kyndryl security controls and best practices. Client specific exceptions for the EDR configuration can be considered through service requests.

SD-3.2.3. Security Information and Event Management

Kyndryl will perform Security Information and Event Management services to collect and store security and audit logs for its management infrastructure only. SIEM implements monitoring, correlation of events, notifications, analysis and reporting of log data.

SD-3.2.4. Vulnerability Scans

Kyndryl will perform routine vulnerability scans on its management infrastructure and the Client's servers under Kyndryl management. Client will be notified if an identified risk vulnerability requires Client's immediate attention. Notice of such risk vulnerabilities may include a cure period allowing Client time to resolve the vulnerability. Kyndryl can suspend Service if Client is unable to or does not cure the risk vulnerability in the allocated timeframe or if such risk vulnerability might cause imminent threat or harm to the Kyndryl network or use of Kyndryl Services or network by unauthorized people.

SD-3.2.5. Data Encryption

Encryption of Client data at rest is enabled on IaaS environments if available from the IaaS provider.

SD-3.2.6. Host Intrusion Prevention System

Kyndryl will implement and manage the Host-based Intrusion Prevention System and will monitor and respond to events generated by the HIPS solution. This service is included as standard for all internet-facing Client systems, according to Kyndryl security controls and best practices. Client specific exceptions for the HIPS configuration can be considered through service requests.

SD-3.2.7. Client Audit Privileges

Client or Client-sponsored third-party audits of the Service or functions related to the Service are not permitted unless expressly authorized in writing by Kyndryl. Client may request an audit in writing to Kyndryl through a service request ticket. All desired audit points should be defined in the request for review. Client is required to execute a separate agreement with Kyndryl establishing the rates, terms and conditions under which Client or its third-party auditor are entitled to audit a Service, functions related to the Service or Kyndryl facilities.

SD-3.2.8. Server Patch Management

Updates and software patches for operating systems are applied automatically via scripts during agreed scheduled maintenance windows. Kyndryl will provide notice either through the Change Requests that can be queried using Portal or through email notification by the Delivery Partner Executive (DPE) of a planned update or available patch in advance of the Scheduled Maintenance window.

SD-3.3. Data Protection

Kyndryl, its affiliates, and contractors of either, may access and use the content solely for the purpose of providing and managing the Cloud Service. Kyndryl will treat all content as confidential by not disclosing content except to Kyndryl employees and contractors and only to the extent necessary to deliver the Cloud Service.

SD-3.4. HIPAA

The Services described in this Service Guide may be expanded with additional security controls to allow for hosting Client's business applications with content regulated under HIPAA (Health Insurance Portability and Accountability Act of 1996).

Client data that includes protected health information (PHI) must be encrypted at rest. Encryption can be requested or done by the Client in their Oracle applications.

Off-device collection and retention of system logs from Client environments and monitoring by Kyndryl security personnel of actions taken by Kyndryl system administrators that have privileged access to Client environments are HIPAA requirements. These security controls must be added to the Services. Automated monitoring using a SIEM application and manual monitoring through random sampling of system logs are available options.

Applications Management for Oracle on Any Cloud is enabled for HIPAA requirements with Information Security Controls which are described in the 'Kyndryl Services for Managed Applications Information Security Controls' Document. Clients are responsible for determining that the Services with Information Security Controls and additional security controls provided by Kyndryl are satisfactory for their business and regulatory compliance requirements. Kyndryl will execute a Business Associate Agreement (BAA) with Client as specified under HIPAA.

SD-3.5. FBA

The Services described in this Service Guide may be expanded with additional security services to allow for hosting content for Clients that are regulated by the FBA (Federal Banking Agencies).

Monitoring by Kyndryl security personnel of actions taken by Kyndryl system administrators that have privileged access to Client environments is an FBA requirement. This security control must be added to the Services. Automated monitoring using a SIEM application and manual monitoring through random sampling of system logs are available options. System security/audit log records used in support of the privilege monitoring requirement must be retained for a minimum of 180 days. Also, the Security Health Checking frequency for FBA-regulated systems must begin no later than 3 months after the previous Security Health Check.

Applications Management for Oracle on Any Cloud is enabled to address FBA requirements with security services described in the 'Kyndryl Services for Managed Applications Information Security Controls' document plus the two additional security services (noted above) to allow for hosting content for Clients that are regulated by the FBA. Clients are responsible for determining that the Services with additional security controls provided by Kyndryl are satisfactory for their business and regulatory compliance requirements.

SD-3.6. PCI

The Services described in this Service Guide may be expanded with additional security services to allow for hosting content for Clients that are regulated by the PCI DSS (Payment Card Industry Data Security Standards).

Applications Management for Oracle on Any Cloud (OCI) is enabled to address PCI requirements with security services described in the ‘Kyndryl Services for Managed Applications Information Security Controls’ document to allow for hosting content for Clients that are regulated by the PCI DSS.

The Management Infrastructure devices running on Kyndryl OCI Cloud Accounts and IBM Cloud Accounts are PCI Certified with yearly PCI Assessments by Kyndryl. The determination on whether PCI Certification is required for Client infrastructure devices running on Client OCI Cloud Accounts is the responsibility of the Client. Clients are responsible for determining that the Services provided by Kyndryl are satisfactory for their business and regulatory compliance requirements.

SD-4. Connectivity

SD-4.1. Client dedicated Virtual Private Cloud/Virtual Cloud Network

Kyndryl will create and manage one virtual private network/virtual cloud network environment into the Client account. Additional private networks/cloud networks can be added at an additional charge.

SD-5. Client Networking

The Client Networking functions are implemented using available, virtualized or dedicated network infrastructure provided by the IaaS provider.

SD-6. Managed Servers

The server functions listed below are implemented using an integrated, highly available, virtualized computing infrastructure. Compute services can be used with available Networking and Storage options. Service supports virtual configurations.

Kyndryl maintains a library of certified server operating system, middleware and application software configurations, including configurations supporting Oracle™ certified workloads. These certified configurations are used to build and deliver Applications Management for Oracle on Any Cloud.

SD-6.1. Virtual Machines

Virtual machines are managed virtual devices configured with virtual core processor units (vCPUs/oCPUs) and virtual memory. As part of the offering, Kyndryl may deploy virtual Images to support the agreed solution on the vendor IaaS. Virtual Machine configurations are defined by the IaaS provider and Kyndryl will use the accepted configurations for Oracle as defined by the provider and Oracle.

SD-6.2. Server Management Options

Applications Management for Oracle on Any Cloud provides standard options for server management.

SD-6.2.1. Operating System Management

Kyndryl will provide operating system administration, troubleshooting and access management. Client access to the operating system will be provided using a strict least access required approach. Client is required to specify the number, type of operating system and configuration of the virtual machine instances. Use of operating system software is subject to acceptance by Client of software license terms. A Project Change Request (PCR) is required to instantiate a new virtual machine or change an existing virtual machine.

Client is responsible for managing Client applications not included in the service scope; this service is meant for bolt-on applications and other 3rd party applications not covered by Kyndryl Services for Oracle Applications Management.

If operating system failure occurs and Client has not ordered any data backup services, Kyndryl will work with the IaaS provider to return the server or virtual machine to the latest certified operating system Image (rebuilds) when necessary. Service includes a maximum of two rebuilds per server per year. Additional rebuilds will be charged at time and material rates. Rebuilds restore certified operating system only and do not restore Client data, applications or application configuration.

Kyndryl provides proactive monitoring of managed operating systems. Kyndryl will provide Clients with notification of Severity 1 events related to operating systems. Kyndryl will monitor and manage the Kyndryl-supported operating systems and will provide Client with electronic notifications.

Alarms and/or events are generated per predefined usage thresholds assigned to each component being monitored; thresholds are set by default and can later be modified. Client is provided access to near-real time and historical reports for each monitored parameter, alarms and/or events. Alarms or events are available through the Portal to view.

SD-6.2.2. Server/VM/OS Management for Database, Middleware and Applications

For servers used in managed database, middleware and application services environments, Kyndryl manages and proactively monitors the availability, performance and recovery of its Kyndryl managed reference operating systems. Kyndryl provides service reports, change request, incident reporting and communications tools to Clients through the Portal. Kyndryl retains exclusive administrative access to the Service platform. Service does not include admin or privileged user access to operating systems to the clients.

SD-6.2.3. EU Labor

As a standard option at additional cost, Kyndryl can provide European Union (EU) based labor services for “OS and above” support to the Client. This option provides EU based personnel for the areas of operating system support.

SD-6.2.4. VM/Server Configuration

Kyndryl will work with the Client to deploy Oracle and IaaS resources and configurations to support the agreed solution.

SD-7. Managed Storage

Kyndryl will provision storage on the public IaaS environment as recommended for Oracle deployments by the vendor and as needed to support Client’s defined sizing requirements.

SD-7.1. Maintenance

IaaS maintenance of the managed storage infrastructure may require migration of Client data. Kyndryl or Cloud IaaS Provider will notify Client in writing when data migration is necessary to allow a mutually agreeable maintenance window to support maintenance activities. Clients will need to notify Kyndryl in the event Cloud IaaS Provider informs the Client directly. Additional charges may apply from Kyndryl.

SD-8. Data Protection for Managed Storage

Applications Management for Oracle on Any Cloud provides a number of backup and restore policy options using the IaaS provider’s native cloud backup capability or by deploying a dedicated backup solution within the Client's cloud account as described below. These data protection options are mainly available for file systems provided through the multitenant Managed Storage offerings.

SD-8.1. Backups

SD-8.2. Backup and Restore

Based upon the Managed Service environment, as set forth in the table below, Kyndryl will perform an initial backup once an environment has been provisioned and when an operating system is patched or updated.

Managed Service Environment	OS	File System Backup and Restore	DB Backup and Restore
Full Service – Production	Included	Included	Included
Full Service – Non Production	Included	Optional	Optional
VMs with OS only support *	Included	Optional	Optional*

*For OS only support VMs, backups for database, middleware and applications are not within Kyndryl Managed Services scope.

Kyndryl will perform and store data file backups (process of duplicating the Client's "to-be-backed-up" "Target Data") on cloud provider storage within the data center as described in the backup schedules below. The database backups include the database files (datafiles, control files and redo logs) and the database archive logs.

For OS only support VMs, database and binary/file system backups are not included.
However, for environments where database and binary/file system backups are not included, add-on backup services can be purchased, e.g., Non Production systems. If Backup service is not purchased for non-production systems, recovery/restore is done by cloning the database and binaries from the production environment.

a. The Default Backup Schedule is:

Default Backup Schedule				
	File System Backup		Database Backup	
	Backup	Retention	Backup	Retention
Production	●Initial full ●Daily incremental	●30 days	●2 full per week ●Daily archive logs (3 times a day)	●30 days
Non-Production*	●Initial full ●Daily incremental	●15 days	●1 full per week ●Daily archive logs (3 times a day)	●15 days

*only when the solution includes backups for non-production.

Client may select from the available **Optional Backup Schedules** (Example: Bronze, Silver, Gold) as per Cloud IaaS Provider's Policy. This will override the Kyndryl backup policy as outlined above.

Notes:

1. Any scheduling conflicts between backup and patch management or other maintenance will result in the backup being performed on the next scheduled backup window.
2. Client must review, understand, and acknowledge their responsibilities prior to implementation.
3. Kyndryl Client support team will coordinate backup and troubleshooting with cloud provider.
4. Kyndryl will be responsible for creating additional storage file systems at Client expense using cloud provided infrastructure.

b. For Backup and Restore, Kyndryl will:

Backup and Restore	
Monitor and Manage backup activity	Included
Perform planning, maintenance, and operations for backup and restore	Included
As required and determined by Kyndryl, order additional storage capacity as required in Client Tenancy account for backup and restore,	Included
All backup schedules will be controlled by cloud providers backup service and provider resources availability. Any scheduling conflicts between backup and patch management or other maintenance will result in the backup being performed on the next scheduled backup window	Included
Backup of DR instances	Not Included
Backup data are automatically stored across multiple storage devices spanning across availability domain(s)/zone(s) within the same regions	Included

c. Kyndryl will also:

- provision additional storage for staging backup data.
- configure the backup data from the Object/Archive storage within Client Tenancy.

d. In addition, Client can request for an additional charge, Restore of Files from Backup to have a database created for day-to-day operation/development. The one-time charge for such service is identical to restore of DB.

SD-8.3. Disaster Recovery Options

Client may order the disaster recovery option as an extension to production Oracle environments for an additional charge. Client must provide the order in which they want their systems recovered.

Disaster recovery service includes:

a. recovery of one production application environment workload from one region to another region of same Cloud IaaS Provider, specified by the Client;

b. Kyndryl managed virtual instances, and approved bolt on applications managed by Kyndryl;

c. ongoing management of the disaster recovery architecture; and

d. once a year disaster recovery testing to include all Oracle disaster recovery protected applications as selected by the Client.

Third party connections related to interfaces to the managed Oracle Application Environment (if applicable) will not be included in the annual test.

The disaster recovery solution is designed with a Recovery Time Objective (RTO) of 4 hours for the first Oracle application system. The RTO for subsequent Oracle application systems will depend on the number of systems and sequence outlined in the Client's Disaster Recovery Plan and agreed to by

Kyndryl. The actual achievable RTO for the selected IaaS locations will be determined during the initial disaster recovery test.

Disaster declaration is the responsibility of Kyndryl as per the Disaster Recovery Plan which will be provided to Client following disaster recovery option enablement. The Client contact information and the communication process between Kyndryl and Client is defined in the Disaster Recovery Plan. Disaster Recovery services will begin after the Production Application Environment Go Live Date at a time agreed upon by Client and Kyndryl. Disaster Recovery Objectives will begin after the first test has completed.

SD-8.4. Disaster Recovery Annual Testing

The annual disaster recovery testing is a data-centric testing with a focus on providing Kyndryl managed Oracle application level testing. It will be a non-disruptive limited test and will allow the Client to conduct a controlled test including bringing up the Operating System, performing login tests and validating Oracle applications can be started.

Kyndryl will:

- coordinate a test schedule that includes one test period per calendar year; and
- assign a Project Manager to assist Client with incorporation of Kyndryl tasks into the Client specific Disaster Recovery Plan. The PM will coordinate the technical aspects of the plan and will assist in the following areas:
  (1) temporary stop of connectivity between active (production) and secondary (DR) site, stop binary and database replication to start fail over recovery process;
  (2) configure temporary connectivity for Client DR test accessibility; and
  (3) troubleshooting and resolution of any technical issue in the above area during the execution of the DR test which falls under Kyndryl's responsibility.

Client will:

- recommend the preferred test schedule subject to Kyndryl acceptance;
- develop the overall DR test plan;
- develop Client resource plan for the testing to cover roles and responsibilities;
- coordinate with Kyndryl Project Manager to initiate the DR test and setup the environment;
- conduct the disaster recovery testing within the test period including enablement of the VPN agent; and
- complete DR testing within a 72-hour period.

SD-9. Managed Oracle

Kyndryl provides managed services for Oracle solutions deployed onto virtual or bare metal servers. The Client solution and the architecture is based upon the information provided by the Client or Client's system integrator. The solution and contracted applications are specified in the Pricing Schedule section of the agreement.

Service includes application installation, administration and support for the Oracle environment. Kyndryl will monitor, alert, resolve and restore application events. Kyndryl will apply relevant patches, fixes and updates (on same software version level) and perform data protection and managed backup services (when requested) as defined in the applicable Pricing Schedule.

Optional resilience services are available for increasing Oracle system availability and disaster recovery protection.

Alarms and/or events are generated per thresholds assigned to each application being monitored. Client is provided access to reports for monitored parameters, alarms and/or events.

The performance of the infrastructure supporting the applications may vary based on how the applications are customized by the Client. Should there be a requirement to increase or decrease the architecture, Kyndryl will work with the Client to make necessary adjustments to run the applications for optimal performance. Changes in architecture may result in pricing changes (either of Kyndryl services or IaaS services) and will be handled through change control procedures.

Oracle implementation and Support processes will be provided along the specified distribution of Responsibility, Accountability, Consulting, and Inform (RACI) table specified in the applicable Pricing Schedule.

SD-9.1. Oracle Service Packages

Oracle services are provided as packaged services and charged on a per-environment basis.

SD-9.1.1. Oracle Full Service

As per the agreement, Kyndryl will provide managed services up to the application layer for Commercial Off-the Shelf (COTS) Oracle packaged application solutions. For non-Oracle and custom applications integrated with standard Oracle packaged applications, Kyndryl can provide managed services up to database or middleware layer.

SD-9.1.1.1. Application Services

This service package provides a comprehensive, best-practice Oracle management for Production and Non-Production Application Environments encompassing all services required to provide application level SLAs and a set of regular services as defined in the RACI.

With this option, service level agreements for Production Application Environments apply through the Oracle application technical layer. Additional application services such as functional support, functional upgrades, enhancements, or module implementations can be purchased for additional charges.

SD-9.1.1.2. Middleware Services

Client may order managed services for a set of additional middleware products, provided they are supported by Kyndryl at the time of ordering. For such products Kyndryl will perform installation, ongoing management, and patching. Monitoring is limited to the process monitoring provided at the OS level. Availability SLAs are limited to Standard Availability SLAs on the OS level. A listing of supported middleware products can be found in A2-Supported Software..

SD-9.1.1.3. Database Services

Database services are provided as part of Oracle application management services for single node installations and for IaaS service configurations. Kyndryl will only install and manage the supported versions of the databases. If Client keeps the unsupported versions of databases, then they are excluded from any SLA/SLO.

SD-9.1.2. Oracle OS Environment

This service is applied for VMs supported up to Operating System layer; database, middleware and applications are not within Kyndryl Managed Services scope.

SD-9.2. Production Application Environments

Kyndryl will provide applicable services per Production Application Environment of:

Service	Oracle Full Service	OS Environment
architecture and design of the infrastructure	Included	Included
installation of operational infrastructure according to Kyndryl internal best practices	Included	Included
configuration of the operational infrastructure per Kyndryl standard internal operating procedures	Included	Included
database, or database and application, installation and configuration according to Kyndryl internal best practices and available Oracle guidelines and documentation	Included	Not Included

For Production Application Environments, Kyndryl will provide applicable services according to the ordered Service Package:

Service	Oracle Full Service	OS Environment
installation of Oracle Applications	Included	Not Included
monitoring for Oracle Applications	Included	Not Included
management of the databases, performing periodic reorganization, resolving database related issues and update management. (Limited to 5 table reorganizations per quarter per Production Application Environment)	Included	Not Included
Oracle Applications patches per RACI	Included	Not Included
Oracle system and Client management	Included	Not Included
Oracle output management (10 printers)	Included	Not Included
Oracle online support services management	Included	Not Included
Client can request up to four Oracle support pack stack patches per year. Client is responsible for all functional testing. Application of enhancement packages is not included and may be provided under a separate mutually agreed to scope and charges	Included	Not Included

Further details of the managed services provided for Production Application Environments are listed in the Kyndryl Services for Managed Oracle Applications RACI.

Client may request a new or existing VM be provisioned and operated the time zone of the IaaS availability domain(s)/zone(s) where the VM is located, not using Universal Time (UT) as is the standard at time of provisioning. Client understands that altering the time zone from UT may cause unexpected results and that VM outages are excluded from any SLA calculation if the root cause lies with, or is exacerbated by, the use of a time zone other than UT. Client accepts full responsibility for risks which may be incurred related to altering the time zone from UT. This applies at initial provisioning or any subsequent reboot of a VM that alters the time zone from UT.

SD-9.3. Non-Production Application Environments

Non-Production Application Environments may be used for development or quality assurance systems or additional sandbox systems to seamlessly support an Oracle application project development implementation phase prior to an Oracle production Go-Live or to support production application environments after Go-Live. Kyndryl will provide applicable services of:

Service	Oracle Full Service	OS Environment
architecture and design of the infrastructure	Included	Included
installation of operational infrastructure according to Kyndryl internal practices	Included	Included
configuration of operational infrastructure per Kyndryl standard internal operating procedures	Included	Included
database, or database and application, installation and configuration according to Kyndryl internal best practices and available Oracle guidelines and documentation	Included	Not Included

For Non-Production Application Environments, Kyndryl will provide applicable services according to the ordered Service Package:

Service	Oracle Full Service	OS Environment
Installation of Oracle Applications	Included	Not Included
management of the databases, performing periodic reorganization, resolving database related issues and update management. (Limited to 5 table reorganizations per quarter per Production Application Environment)	Included	Not Included
Oracle Applications patches per RACI	Included	Not Included
Oracle system and client management	Included	Not Included
Refresh/clone existing Oracle target systems from separate Oracle source systems using homogeneous system copy (Database Refresh) or refresh existing clients with Remote Client Copy if database is less than 1 TB. Kyndryl will perform 1 refresh or clone per month per Oracle Applications upon Client request. Additional refreshes and clones can be requested for an additional charge.	Included	Not Included

Further details of the managed services provided for Non-Production Environments are listed in the Kyndryl Services for Managed Oracle Applications Responsibility Matrix (OS and Oracle Services).

SD-9.4. Optional Services – General Service Extensions

The following optional services may be ordered for additional charges and will be managed using the change control process.

a. Oracle Applications Add-ons

b. Oracle Support package Stack

Application/patching of Support package Stacks and Technical Support package Stack above any included entitlement per Oracle Service Package

c. Database Refresh or Cloning

Homogenous DB refresh of cloning including pre and post tasks. Oracle System ID (SID) of existing systems remain unchanged

d. Clustering services

Provide setup and management of a cluster service for database servers and Oracle Application servers to provide high availability or automated failover of the clustered server to a standby server.

e. High availability SLA

This service provides a separate high availability commitment with associated service charge credits. It can be ordered for clustered systems that span different IaaS fault domains/zones and/or availability domains/zones.

f. Application/database monitoring for non-prod environments

When monitoring is enabled for non-prod environments, they will be considered 'controlled environments'; change control policies including lead time for changes will be applied to the controlled environment.

g. Install and configure Secure Socket Layer (SSL)

h. Interface server, if applicable

SD-9.5. Miscellaneous One Time Services

The following services are available for selection by Client on a per-use basis. Client can request the following Services via an Order Document/Service Request.

a. DB refresh or cloning (homogeneous system copy)

DB refresh of cloning is a Service Client can use to request creation of a duplicate of an Oracle system from a source. The operating system and database platform are the same for both the source and target system. During the system copy, certain Oracle parameters are changed. The one-time charge for the service is per system copied.

b. Oracle Additional Language Installation

Each Oracle system is installed in English by default. Further languages packages can be requested to be installed on demand.

c. Additional Backup of Oracle Application environment

Services to create an additional backup above the standard backup policy.

d. Client-initiated Restore from backup

Client requested service to restore a system from a defined backup.

e. Enable Additional Currency

f. Code Migration – For every 5 migrations per month

g. Setup up to 10 additional printers

h. Application Performance Analysis

i. Database Performance Analysis

j. System Performance Tuning (OS and below)

k. Additional Oracle DR Test Execution per Application

Provides execution of a Disaster Recovery test for One Oracle Application environment in scope. One yearly test is required to maintain validity of recovery time and recovery point objectives defined for Disaster Recovery services.

l. Change of IaaS VM type for 1 Instance

Provides the services to change the underlying IaaS VM configuration for 1 managed system following the defined change management process for this system.

m. Oracle System Shut down

Provides the services to shut down and keep 1 managed Oracle Application environment following the defined change management process for this system.

n. Oracle System Restart within 1 Month

Provides the services to restart 1 managed Oracle Application environment within 1 month following the previous shut-down.

o. Oracle System Restart after more than 1 Month

Provides the services to restart 1 managed Oracle Application environment later than 1 month after the previous shut-down.

SD-9.5.1. Data Migration

If Client orders data migration services, Kyndryl will provide project management and implement the plans, processes and tools to perform data import of Client’s existing Oracle production application environment to a Managed Service Oracle Application Environment to meet steady state architecture, processes and service level agreement, and standards.

There are limitations for this service with regard to size of data (less than 4TB for heterogenous data load and less than 6TB for homogeneous data loads) and a system downtime of 48 hours is required for this service. In case the size is exceeded or the downtime is not acceptable, a separate custom database migration project can be ordered at an additional custom charge.

SD-9.5.2. Additional Support Services

Kyndryl can provide any additional Oracle Application transformation services to support both establishing a new managed environment or migration of existing Client environments to a Managed Service environment as mutually agreed scope.

SD-10. Kyndryl Client Support Services

SD-10.1. Client Onboarding and Implementation

Kyndryl will provide onboarding and implementation services for the infrastructure and applications as defined in the applicable Schedule. Onboarding and Implementation services include project management, project planning and assistance with the preparation of the environment at the Service Location in support of the Services. Following execution of the Schedule, Kyndryl will coordinate a conference call with Client’s program sponsor to prepare for the project. During the conference call, Kyndryl will:

- Review and confirm project objectives, scope and approach;
- Establish project timeline, schedule and milestones;
- Review project assumptions;
- Review Client-provided documentation and diagrams supporting the Services;
- Provide a questionnaire, to be completed by Client, which is required for Client specific information such as installation requirements (e.g., database release, OS version, etc.) to order a Managed Service environment;
- Notify Client when an Environment is ready for data load (the Service Ready Date); and
- Provide Client’s authorized contact with required information and access identification (IDs).

Onboarding and Implementation Services can also provide:

- Support during the preproduction implementation stage;
- Development and implementation of operations readiness test and cutover procedures prior to the management being transitioned to lifecycle support teams; and
- Technical support to assist with Client’s application deployment.

A project plan will be developed which will define the activities required to install the infrastructure and applications.

Client is required to:

- Assign a single point of contact to ensure ongoing Client focus and support.
- Provide a single point of contact that will work with Kyndryl to coordinate scheduling and logistical support;
- Provide technical resources to assist with the implementation of the Services;
- Provide an access list of persons authorized for: access, opening trouble tickets, scheduling maintenance, and requesting changes;
- Identify those employees authorized to request modifications to the access list;
- Provide timely access to and participation of Client personnel during implementation activities, in accordance with the schedule mutually agreed upon; and
- Monitor usage and coordinate, manage, and educate users for compliance with the terms applicable to the use of the Managed Service.

When Client contracts IaaS Infrastructure directly with IaaS approved vendor, Client is required to:

- Obtain and pay for IaaS account with the agreed vendor and then grant Kyndryl full rights to use the account as needed to deploy Client services;
- Pay in full the charges from IaaS on the agreed IaaS schedule;
- Work with Kyndryl to define reserve usage for VMs;
- Provide and keep current any required valid funding authorization, such as a purchase order, if Client requires any such authorizations for Kyndryl to invoice charges; and
- For Client owned elements, work with Kyndryl to develop a communication plan for Client delivery and if applicable supply solution documentation.

SD-10.1.1. Ordered Environments

For each environment Client orders, Client will specify if the environment is for production use or non-production use. A Production Application Environment is used by Client or its users in support of Client’s ongoing business operations to run production workloads. A Non-Production Application Environment may be used for other purposes such as development, testing or training and is not used for production workloads. The minimum term that can be selected for a Non-Production Environment is one month. The minimum committed term for a Production Application Environment is identified in the Order Document. Additional charges may apply if a Non-Production Application Environment require additional or dedicated hardware. Kyndryl may use Client's Non-Production Application Environment for troubleshooting or other testing required to resolve an application problem or test and apply an update. During such time Kyndryl will have priority use of a Non-Production Application Environment.

To begin production operations of an initial Application Environment or after the introduction of new application functionality, upgrade or significant change in the architecture of an Application Environment, a stabilization period to resolve any remaining implementation issues will begin. Client and Kyndryl will mutually agree upon the end of a stabilization period (no less than 30 days). No service levels agreements apply during any stabilization period.

Kyndryl will control all access above the operating system for each Application Environment. Kyndryl will provide Client with appropriate access permissions necessary to enable Client to perform Client responsibilities and administrative functions for the specific ordered Managed Service environment as set forth in the Kyndryl Services for Managed Oracle Applications Responsibility Matrix (Oracle Services). Client will not be provided administrative access to OS on Oracle Application Environments in the infrastructure.

SD-10.2. Test and Turn-Up of the Managed Services

Kyndryl will perform system validation testing of Kyndryl-managed Service Components in conjunction with Kyndryl test schedules prior to transition to lifecycle support by:

- Validating that Kyndryl managed infrastructure and applications are operational and subject to Kyndryl monitoring;
- Validating that noncertified or uniquely configured software is operating according to Client specifications as defined in the applicable Schedule;
- Document and audit environment controls, devices and configuration to verify operational readiness;
- Apply quality assurance methodology to environment including redundancy testing and startup/shutdown procedures including supported applications as contracted; and
- User acceptance testing prior to environment go live.

To allow Kyndryl to complete system validation testing, Client shall:

- Coordinate testing in conjunction with Kyndryl test schedules;
- Provide additional information or documentation relating to Client managed elements within overall service design as required to allow Kyndryl to complete testing; and
- Provide user acceptance testing prior to environment go live.

SD-10.3. Cutover of Production Traffic

Upon notification from Kyndryl of production and lifecycle support readiness, Client is responsible for redirecting Domain Name System (DNS) entries from the existing sites/services (if applicable) to the Kyndryl-supported IP addresses. When necessary, Kyndryl will validate the DNS redirection.

SD-10.4. Client Service Management

Client Service Management is led by two primary Kyndryl leaders:

- Client Partner Executive (CPE) owns the overall contract and associated relationship with Client. The Client Partner Executive has the primary role of executive advocate for all matters pertaining to the contract as well as the Strategic Governance model.
- Delivery Partner Executive (DPE) is responsible for oversight and facilitation of all operational aspects of service delivery. The DPE is a primary point of contract for any issues or needs associated with Kyndryl's service delivery performance. The DPE can be a unique regional resource dependent upon contracted region.

Client Service Management provides for multiple Client experiences by aligning Clients to one of three Service Tiers: Basic, Advanced or Premium. These tiers are designed to reflect the scale of management required by Client and expected volumes of Client-initiated monthly Service Requests and Change Requests (Service Plans). Each Service Plan is 10 Change Requests or Service Requests per calendar month as requested by Client.

Additionally, each tier entitles Client to service features that will further enhance the Client's experience.

		Service Tier		
		Basic	**Advanced**	**Premium**
Monthly Entitlement	Incidents and Ticketing	Uncapped	Uncapped	Uncapped
	Baseline Service Plans	1 Service Plan	2 Service Plans	3 Service Plans
	Offering(s)	Managed Application Services	Managed Application Services	Managed Application Services
Onboarding & Readiness	Onboarding	Onboarding Project Manager	Project Integration Manager	Project Integration Manager
	Service Readiness	Managed Application Services	Managed Application Services	Managed Application Services
Case Management	Severity 1 Incidents	Escalations via Portal	24x7 by On Call Managed Escalation Support for Production Environments	24x7 by On Call Managed Escalation Support for Production Environments

		Service Tier		
		Basic	Advanced	Premium
	Severity 2 Incidents	Normal Business Hours via Portal	24x5 (Monday through Friday) by On Call Managed Escalation Support for Production Environments	24x5 (Monday through Friday) by On Call Managed Escalation Support for Production Environments
	Severity 3 Incidents	Normal Business Hours via Portal	Managed during Normal Business Hrs.	Managed during Normal Business Hrs.
	Support for Change Management	As needed on a twice a month basis	Managed weekly in collaboration with Client change controls Process	Managed weekly in collaboration with Client change controls Process
	Language Support	Standard: English	Standard: English	Standard: English
Governance	Operations Review	None	Weekly	Weekly
	Monthly Measurements Review	None	Review of Key Service Metrics and ongoing projects	Review of Key Service Metrics and ongoing projects
	Quarterly Business Reviews	None	Joint Executive Business Strategy and Innovation Topics	Joint Executive Business Strategy and Innovation Topics

If Client exceeds Service Plan entitlement as reflected in the Schedule in any calendar month, Kyndryl shall reserve the right to charge Client for additional Service Plans consumed.

Kyndryl may recommend Client contracts for additional Service Plans for fulfillment of Kyndryl-identified Client trends. For avoidance of doubt, Change Requests and Service Requests accounted for in each Service Plan shall not include Client tickets raised outside the Change Management Process and Service Request management process.

Clients subscribing to Basic, Advanced, or Premium Service Tier:

- may request local languages DPE support provided Kyndryl has in-region personnel that speak the languages requested by Client; and
- may order Ad-hoc services such as additional disaster recovery planning for additional charges.

SD-10.5. Service Desk

Kyndryl will set up and manage a service desk. Only authorized contacts from the Client will be authorized to contact the Service Desk. The Client’s authorized contacts can submit and track Severity 1, 2, and 3 incidents online via the Kyndryl provided portal, which is available 24 x 7.

Authorized contacts are required to have a sufficient level of understanding with respect to the application, Client's business processes and Kyndryl's Service Request management processes to enable accurate communication of Incidents/problems and reasonably assist Kyndryl in troubleshooting. Kyndryl's Service Desk cannot be integrated with Client's ticketing system. All service desk communication will be conducted in the English language, except when Client purchases Japan Help Desk Services, which allow communication in the Japanese language.

SD-10.6. Japanese Service Desk

Client may order Japanese service desk support for an additional charge. Kyndryl will:

a. receive requests for ticketing by email from Client's authorized contacts;

b. open tickets on behalf of Client;

c. track the ticket status;

d. report status to Client's authorized contact; and

e. translate Japanese to/from English for any communication between Client and Kyndryl.

Service hours are Monday through Friday 9:00 AM to 5:00 PM (excluding Japanese national holidays) Client local time. Japanese service desk cannot be integrated with Client's ticketing system.

SD-10.7. Technical Support Service Hours

Kyndryl will provide Oracle Application and DB administrative skills with specific knowledge about the Client Application Environment to provide the in scope services. All related communication is in English, except when Client purchases Japan Help Desk Services, which allow communication in the Japanese language.

Production	Non-Production
24 Hours * 365 Days for all Production Application Environments	Weekdays local to the Client (8 am – 6pm)

SD-10.8. IaaS Portal

Where necessary, allow Kyndryl to provide monitoring and management of Services to Client, Client authorizes Kyndryl to access Client information using the IaaS portal.

SD-11. General Terms

SD-11.1. Client Orders for Service or Service Components

To order Services, Kyndryl and Client will develop a technical service definition form that contains the technical details necessary to provision services at an IaaS provider DC that constitutes the physical and virtual computing, storage and network services used to run software operating systems and applications.

Client is required to provide all technical details necessary to identify Service components required before Services may be provisioned.

When Client procures IaaS Infrastructure from an IaaS approved vendor, Kyndryl does not own or retain any ownership of the IaaS infrastructure or software from before to after the contract ends. Client gives Kyndryl explicit rights to launch the relevant resources needed to perform its duties while under contract. Kyndryl requires no prior approval other than the acceptance of this document to launch the necessary devices on the Client account. Client agrees to pay in full the monthly fees from the IaaS provider, including any bandwidth charges. If disputes arise, Kyndryl will work with the Client to resolve billing or justification for billing, however Client indemnifies Kyndryl for any IaaS payments unless negotiated.

Along with paying for IaaS services, Client also agrees to pay Kyndryl for all Kyndryl Services for Oracle Applications Management on multiple cloud environments charges. These charges will be set forth in the charge schedule and will be provided to the Client at the time of signing.

Following Client's original Order and Pricing Schedule, a Service Request for additional Service features may be made via an additional Order and Pricing Schedule or (if available via a portal. All orders are subject to the terms of the Agreement, and Client agrees to pay for any such Services.

Client may not resell direct access to any of the Services to any third party without entering into a separate agreement with Kyndryl. Client is responsible to have appropriate agreements in place with Client's Solution Recipients, including rights to process content requested or provided by Client or Client's Solution Recipients, and is responsible for their use of a Client Solution.

SD-11.2. Services Changes

Kyndryl may from time to time add new Services or options, or in its reasonable discretion, withdraw existing Services or options, in whole or in part as set forth below:

1. For changes to existing Services or options described in this Service Guide, Kyndryl will notify Client of any new or changed Services and the effective date of such by providing notice directly to a Project Executive using current information in Client's Account.
2. For any change that affects existing Services, but is not a withdrawal of the Service as specified in paragraph 3 of this SD-11.2, the change will be effective the later of i) 90 days after the date of the notice; ii) the specified effective date; or iii) as may otherwise be specified.
3. For withdrawal of the Service in its entirety, Kyndryl will provide Client with one hundred eighty (180) days' notice.

SD-11.3. Acceptance of Changes

Client acknowledges its agreement to any of the above changes by i) continuing to use or ordering Services after the effective date of the change, ii) allowing Services to renew after receipt of the change notice; or iii) by signing (in writing or electronically, where permitted) an applicable revised Order and Pricing Schedule or other change authorization mechanism Kyndryl may provide (such as on-line acceptance).

SD-11.4. Services Rates, Billing and Service Activation

Billing for Service shall be on a nonrecurring (one-time), and monthly recurring basis. Billing for Service or Service Component begins on the date(s) specified in the Schedule.

Commitments, enhancements, and options selected by Client and actual usage will affect the total charges Kyndryl will invoice.

Client will be invoiced monthly beginning on the first day of the month following the Service Activation Date. Client agrees that the charges stated in a signed Schedule will apply to all Services ordered, are payable in the specified currency, and are exclusive of any duty, tax, levy or fee. Client understands that Kyndryl may from time to time add additional Services or options and make them available to Client to order at current market prices.

Kyndryl will invoice applicable charges as follows:

- usage charges will be billed at the end of each month based upon actual use of Services multiplied by the specified unit charge;
- recurring charges will be billed at the end of each charge period (e.g., monthly, quarterly or annually) and will be prorated based on when such Services begin or end; and
- one-time charges will apply when such Services are delivered.

During the term of this Agreement, the amount of charges set out in the applicable Order and Pricing Schedule may be modified to the extent of:

- any adjustments due to a Change Request mutually agreed by the Parties; or
- any adjustment in the rates or charges imposed by an applicable third party supplier of a component of the Services, provided that Kyndryl will notify Client in writing of the corresponding change to Kyndryl’s rates at least thirty (30) days prior to the effective date of Kyndryl’s rate change.

In addition, for early termination by Client, Termination Charges as per the Schedule may apply and will be billed upon the closing of Client’s Account.

Client will reimburse the travel and out-of-pocket expenses that Kyndryl incurs in performing the Services and which have been pre-approved by Client in writing. Kyndryl may charge late payment fees at the lower of 2% per month (24% per annum) or the maximum rate allowed by law for overdue payments.

Any requests for additional services may be submitted to Kyndryl in accordance with the Changes section of the Schedule.

SD-11.4.1. Service Activation Date

For all Kyndryl managed Services or Service Components, the Service Activation Date for the Services or for the individual Service Component(s) is the implementation date.

The implementation date for operating system server management Services is the date when the infrastructure and applications for Client service is installed by Kyndryl and supplied with network connectivity, regardless of whether Client managed content or software applications have been deployed by Client.

For Application Services Clients with advanced managed servers or other Services or Service Components, the implementation date is when Kyndryl provides notice that the Service is available for use or the date on which a Client or user begins using the Service or Service Component, whichever date is earlier.

SD-11.4.2. Client Delay of Service Activation

Any delay in performance of Client’s responsibilities may result in additional charges and/or delay of the completion of Services or Service Components and will be handled in accordance with the Changes process specified in the Order and Pricing Schedule**.**

SD-11.5. Termination or Cancellation of Services or Service Components

SD-11.5.1. Termination of Services or Service Components

Client may terminate Services or Service Components after the Service Activation Date as specified in the Schedule by (1) providing not less than sixty (60) days prior written notice; (2) paying for all Services and Service Components provided up through the effective date of termination; and (3) paying all disconnection, deinstallation and applicable termination charges, as described in the applicable Schedule.

SD-11.5.2. Withdrawal of Services or Service Components

Unless expressly otherwise provided in the Agreement, and unless applicable law or regulation mandates otherwise, Kyndryl may discontinue providing the Services upon 180 days’ notice or a Service Component upon 90 days’ notice to Client, but only where Kyndryl generally discontinues providing the Services or Service Component to similarly situated Clients.

SD-11.5.3. Return of Content

Not later than thirty (30) days after expiration or termination of the applicable Product Exhibit, Kyndryl will, at Client's expense, return the Client Content in Kyndryl's possession or control after the removal of any applicable Kyndryl IP. For the sake of clarity, if Client requires Content to be provided on a specific media, additional charges may apply.

SD-11.6. Availability Domain(s)/Zone(s) Location

Kyndryl utilizes multiple Cloud IaaS Providers' availability domain(s)/zone(s) locations to deliver the Services.

Client VMs are provisioned, stored, and delivered into Client's specified account with agreed IaaS provider and to the Client specified locations. Not all Services and options are available in all Cloud IaaS Provider's availability domain(s)/zone(s).

SD-11.7. Third Party Software License Rights and Restrictions

Client will retain all its rights, title, and interest in and to Client content. Client content and the Services may contain confidential information and other valuable proprietary information. Neither party, directly or through a third party, will alter, copy, reverse engineer, decompile, disassemble, attempt to derive source code from, license, sell, transfer, lease, disclose, or modify or remove any copyright or proprietary notice, from Client content (in the case of Kyndryl) or from the Services (in the case of Client). Client also will comply with all third-party license terms for Client software.

Services may contain software licensed by Kyndryl or licensed by third party software providers. Specific terms below may apply depending on the software licensor, and in addition third party software and its use will be licensed in accordance with the applicable third-party license agreement ("Third-Party Agreement"). The Third-Party Agreement is an agreement between Client and the third-party software owner or rights holder only. Kyndryl is not a party to any such Third-Party Agreement. Client receives no warranties, indemnities or express or implied patent or other license from Kyndryl with respect to any third-party software. Kyndryl's provision of Services hereunder does not constitute a distribution of the third-party software by Kyndryl.

SD-11.7.1. Client Provided Software

Client is permitted to bring and upload its own properly licensed non-operating system software (BYOSL) for use within the Services by installing it directly on a VM. Client is responsible to ensure Client has the necessary licenses, entitlements, and approvals for adding, installing, uploading, transferring, and using such software with the Services.

For any Client provided Microsoft software, Client shall ensure that any BYOSL Microsoft software uploaded by Client to a VM in the Any Cloud environment is covered with licenses / software maintenance (if required) which are adequate in type and sufficient in quantities to comply with Microsoft's license requirements and that they are eligible to be used in a multi-tenant cloud environment.
Client agrees to reimburse Kyndryl for any reasonable costs and other amounts that Kyndryl may incur from Client's failure to obtain these licenses or approvals.

Services are provided from a shared, multi-tenant environment operated by Kyndryl as a service provider. The following provisions apply to any BYOSL non-operating system software licensed to Client by Microsoft Corporation or a Microsoft authorized reseller.
For the purposes of this provision, "License Mobility through Software Assurance" means the rights described in the section titled "License Mobility through Software Assurance" in the Microsoft Product Use Rights. The Microsoft Product Use Rights are located at: https://www.microsoft.com/licensing/software-assurance/default.aspx or a successor site.

In order to exercise License Mobility through Software Assurance rights, Client must, prior to uploading any Microsoft software as BYOSL to a VM in the Any Cloud environment, execute the "Mobility Verification Form" located at: https://www.microsoft.com/licensing/software-assurance/license-mobility.aspx or at a successor site and submit the completed Mobility Verification Form to Microsoft for verification.

Microsoft will provide Kyndryl and Client with confirmation of Client verification status to exercise the License Mobility through Software Assurance Product Use Rights, and the specific products and license counts Client will be authorized to deploy in the Any Cloud environment. This information may be used to support compliance reviews and discussions.

If Kyndryl or Microsoft believe in good faith that Client is not complying with the terms of License Mobility through Software Assurance, as described in the Product Use Rights, Client must cooperate in good faith with Microsoft or Kyndryl to investigate and remedy any potential non-compliance. If requested by Kyndryl and/or Microsoft, Client agrees to provide any additional and reasonable information to support the investigation and remediation, if any, of the non-compliance.

If Microsoft determines that Client is non-compliant with the License Mobility through Software Assurance program requirements, Microsoft will provide Client with written notice of the non-compliance which will include an itemization of the non-compliant issues. Client will work with Microsoft to resolve the Client's status and determine if termination can be avoided. If the parties are unable to achieve a mutually agreeable resolution, Microsoft will provide Client and Kyndryl with written notice to terminate the benefits of License Mobility through Software Assurance for Client. Upon receipt of such notice, Client will promptly remove the instances provided in the notice and utilized by Client and provide written notice to Microsoft with a copy to Kyndryl.

Software may be issued by the IaaS provider in support of the Kyndryl Managed Service. Such software may be provisioned by Kyndryl using IaaS provider portal or APIs and will be invoiced directly to Client by the IaaS provider or by Kyndryl when Client is procuring IaaS and other cloud services through the Kyndryl Resell Program.

For software Client has licensed separately from IBM Corporation ("IBM Software"), only those that are in accordance with the "IBM Eligible Public Cloud BYOSL Policy", which can be found at this url: https://www-01.ibm.com/software/passportadvantage/eligible_public_cloud_BYOSL_policy.html#eligiblesoftware,

may be uploaded as BYOSL software for use in the Services.

SD-11.7.2. Additional Service Component Software Terms

If Client uses software for which Client does not have proper licensing, Kyndryl may assess additional charges based upon actual use and require Client to obtain proper licensing.

Client understands Kyndryl may be required by agreement with the applicable third-party supplier of software to provide usage data and Entitlement information specific to usage of a third-party Services Component. Client will be responsible to such third-party supplier for any improper use, including additional charges and requirements to obtain additional Entitlements.

Client's use of Services Component Software, governed by the applicable license agreement, which may include license information or other documentation associated with such software, ("License Agreement"). For Service Component Software from the IBM Corporation, applicable license agreements are also available at selecting the option to "search for a specific program license agreement" and then entering the name of the IBM software).

Notwithstanding any terms of a License Agreement to the contrary, the following terms apply to all Service Component Operating System Software, and each SC Software product for which Client brings Client's own existing license, except if otherwise specified by Client's license with the software provider:

- The Services Component is provided for a term set forth in the Agreement and is not perpetual;
- No installation or download by Client of a Services Component, in whole or in part, is permitted except as set forth in the applicable Schedule;
- No copies (including back-up copies) of a Services Component, in whole or in part, are permitted except as specifically set forth in the applicable Schedule;
- No transfer of a Services Component, in whole or in part, is permitted during the term of the Services; and
- Any money back guarantee and warranty that may be provided in a License Agreement may not apply to Services Components.

Services Components may not contain all features or functions of the generally available software available directly from the software licensor.

SD-11.7.3. IaaS Provided Operating Systems

Each server will be provisioned with an Operating System Image (Operating System Software) of Client's selection. Where available Kyndryl will use Operating System Software offered by the IaaS provider for the virtual machines used by Client. Client legacy Operating System Images may not be used in the Service. If software for a supported OS is not available from the IaaS provider, Client will provide sufficient OS licenses for the servers deployed.

For the purposes of this section, Operating System currency means that Kyndryl will support two (2) versions of an IaaS Operating System software, whether the two most recent levels are considered minor or major releases. For purposes of illustration, Kyndryl will support versions 1.4.1 and version 1.4.2, or version 1.4.2 and version 2.0.

Kyndryl will maintain currency of supported Operating System software as follows:

- Minor versions Kyndryl provides (for example, v1.4.1 to v1.4.2) will generally be deployed and supported throughout the VMs within six (6) months of general availability as announced by the software vendor, provided the application and application supporting components, such as middleware and database, are certified by application vendor on the new release;
- Major versions Kyndryl provides (for example, v1 to v2.0) will be generally deployed and supported throughout the VMs within nine (9) months of general availability as announced by the software vendor, provided the application and application supporting components, such as middleware and database, are certified by application vendor on the new release; and
- For any version (minor or major) of the Operating System software that is no longer to be supported by the software vendor, for any reason:
  - Kyndryl will withdraw any such Operating System software from sales no later than six (6) months before the date the vendor has announced that support will no longer be available, if the software vendor provides at least six (6) months' notice; otherwise, the Operating System software will be withdrawn from sales immediately;
  - Kyndryl will provide support to such Operating System software installed on VMs until the day before the date the vendor discontinues its support; and
  - Client accepts full responsibility for risks which may be incurred related to use of Operating System software that is no longer to be supported by the software vendor for

any reason including, but not limited to, risks to the security integrity, availability, and confidentiality of the system, databases, applications, and its data.

Kyndryl may provide update/migration custom services for an additional charge to Client.

SD-11.7.4. Service Component Operating System Software License Terms

Client's use of Services Component Operating System Software is governed by the applicable license agreement ("License Agreement") described in the IaaS provider terms. All software that Kyndryl manages with Kyndryl Services for Oracle Applications Management for multiple cloud environments is licensed under the applicable license agreements available at vendor sites. Client is responsible to ensure they have proper licenses for any software Kyndryl manages.

a. Red Hat Linux server software is licensed from Red Hat under additional license terms to be found at www.redhat.com/licenses/cloud_cssa/.

b. Microsoft Server operating system software product (referred to as "Product" in this section) is licensed from Microsoft and Kyndryl is required to include the following terms and Client agrees to the following:

   - Client shall not remove, modify, or obscure any copyright, trademark or other proprietary rights notices that are contained in or on the Products;
   - Client shall not reverse engineer, decompile or disassemble the Products, except to the extent that such activity is expressly permitted by applicable law;
   - Microsoft disclaims, to the extent permitted by applicable law, all warranties by Microsoft and any liability by Microsoft or its suppliers for any damages or remedies, whether direct, indirect, or consequential, arising from the Software Services. For the purposes of this section Software Services means the services Kyndryl provides to Client that make available, display, run, access or otherwise interact, directly or indirectly, with the Products;
   - Kyndryl may disclose Client information such as the total number of licenses and country of usage, Client name and address;
   - Technical support for the software Services will be provided by Kyndryl or a third party on Kyndryl's behalf (and not Microsoft or its suppliers); and
   - There is a "No High-Risk Use" requirement that the user may not use the Product in any application or situation where the Product(s) failure could lead to death or serious bodily injury of any person, or to severe physical or environmental damage ("High Risk Use"). Examples of High-Risk Use include but are not limited to aircraft or other modes of human mass transportation, nuclear or chemical facilities, life support systems, implantable medical equipment, motor vehicles, or weaponry systems. High Risk Use does not include utilization of Products for administrative purposes, to store configuration data, engineering and/or configuration tools, or other non-control applications, the failure of which would not result in death, personal injury, or severe physical or environmental damage. These non-controlling applications may communicate with the applications that perform the control but must not be directly or indirectly responsible for the control function.

c. Client accepts full responsibility for risks which may be incurred related to use of Operating System software that is no longer to be supported by the software vendor for any reason including, but not limited to, risks to the security integrity, availability, and confidentiality of the system, databases, applications, and its data.

d. Additional rules established by the IaaS provider.

SD-11.8 Auto Renewal

Upon the expiration of the Term, the Service Description will automatically renew for additional one (1) month periods (a "Renewal Term"), and Services will be provided at Kyndryl's then current rates, unless Client or Kyndryl provides written notice to the other of intent not to renew at least thirty (30) days prior to the end of the initial Term.

SLA-1. Service Level Agreements

SLA-1.1. General Terms Applicable to Service Level Agreements (SLAs)

Except where an individual SLA states differently, SLAs and the collection of data measurements against a performance objective shall begin on the 91st day after Service Activation Date.

SLA reporting will be made available to Client in the next complete monthly reporting period.

Except as otherwise stated in an Order and Pricing Schedule, SLAs apply only to production environments.

SLA-1.2. Service Level Agreement (SLA) Exclusions and Limitations

Kyndryl is not responsible for failure to meet an SLA resulting from any of the following events:

- IaaS provider infrastructure failure.
- Negligent conduct or misuse of the Service by Client
- Negligent conduct or misuse of the IaaS Infrastructure by Client
- Conduct of a third-party service provider providing Service to Client
- Failure or deficient performance of power, equipment, network, services or systems not provided by Kyndryl
- Service interruptions, deficiencies, degradations or delays:
    - Due to Client equipment managed by Kyndryl that has not been upgraded by Client as required by Kyndryl
    - Due to failure of content, code or software managed and/or written by Client or a third-party vendor for Client including, but not limited to, content installation and integration
    - During any period when Kyndryl or its agent is prevented from implementing software patches or upgrades necessary for Kyndryl to provide Service
    - During any application failures caused by Client disrupting or adversely impacting its service or failing to respond to alerts as agreed or creating false alerts
    - During agreed upon maintenance windows
    - During any period when a Service Component is removed from service for maintenance, replacement or rearrangement purpose or for the implementation of a Client order
    - Due to an act by Client through the use of root or administrative access to a virtual or physical server including but not limited to system administration, commands, or file transfers performed by Client or its representatives.
    - Due to interruptions caused by a Client-managed Active Directory domain controller, including, without limiting the foregoing, interruptions arising from faulty domain communications, domain policies on the environment, or the security configuration of the domain controller.
    - Due to denial of service attacks, natural disasters, changes resulting from government, political, or other regulatory actions or court orders.

  - Due to (i) Client being aware of a Severity 1 problem that was not already reported but failed to promptly report the problem to Kyndryl or (ii) lack of availability or untimely response time of Client to respond to incidents that require their participation for source identification and/or resolution, including meeting Client responsibilities for any prerequisite Services.
  - Due to Client’s inability to restore the OS from a client backup.
  - Due to Client’s breach of their material obligations under this Agreement or under Client requested deviations from the Kyndryl Services for Managed Applications Information Security Controls policy.
  - Due to Client’s failure to meet Client responsibilities within the Kyndryl Services for Managed Applications Information Security Controls policy.
  - Due to Client’s performance of any technical security integrity review, penetration test, or vulnerability scan pursuant to security obligations set forth herein.
  - Due to periods in which Operating System software that is no longer supported by the software vendor is in use.
  - Due to periods in which the system time zone is set to a time zone other than UT.
  - Due to a stabilization period.
  - Due to incidents related to a Client’s use of temporary software licenses.

- Client’s refusal to allow Kyndryl to perform maintenance deemed necessary to maintain the Service, whether scheduled or unscheduled

- Force majeure conditions

SLA-1.3. Service Level Agreement (SLA) Claims

SLA-1.3.1. SLA Process

Each month Kyndryl will measure SLAs and, where Client is due a remedy, Kyndryl will issue a credit against the ensuing month’s service fees in accordance with this Service Guide. All SLAs start at OS and above.

To be eligible for a Services Credit, Client shall notify Kyndryl in writing of a claim within 10 days of the day Kyndryl failed to meet the SLA performance objective or that Client otherwise became eligible for the Services Credit. Client shall send its claim to an email address specified by Kyndryl. All claims submitted by Client shall include the date and time of the outage or other event that Client believes makes it eligible for a Services Credit. Kyndryl shall, in its sole and reasonable determination, verify and determine Client’s eligibility for a Services Credit.

SLA-1.3.2. SLA Claims Limitations

Excluding the Kyndryl Services for Oracle Applications Management for multiple cloud environments Response Time SLA detailed in SLA-3 below, Client may claim one (1) SLA Services Credit for one (1) affected system per calendar month. In cases where more than one system is affected, Client shall choose which affected system will be subject to the Services Credit. Client will not receive a Services Credit for installation charges, public cloud resell, other monthly recurring charges or charges related to additional services. Any Services Credit paid to Client shall constitute the Client’s sole and exclusive remedy for Kyndryl’s failure to meet an SLA.

SLA-2. Availability Service Level Agreement (SLA)

For Full-Service Package, service level agreements for Production Application Environments apply through the Oracle Application layer. For Non-Production and OS Environment, service level agreements apply only through the operating system layer.

Offer Service Level	Service Level Tier	Availability Metric
Managed Oracle	Standard	99.90%
	High Availability	99.95%

When more than 1 Application Environment is in scope, Availability is calculated for individual Application Environment, and proportionate Services Credit will be applied.

SLA-3. Response Time SLA

Kyndryl offers an SLA for response time. Response Time is measured from the time that Kyndryl receives notice of an incident until the time that Kyndryl responds to Client. “Notice”, as used in this section, refers only to the notification that occurs in electronic form through the Kyndryl provided Portal.

Kyndryl will respond to 100% of Severity incidents during the hours of technical support for the Client per the following:

Label	Definition	Response Time
Severity 1	Incident that prevents all Client use of the Service	within 15 minutes
Severity 2	Incident with significant and materially adverse effect on use of the Service or on Client’s key business processes	within 3 hours
Severity 3	Incident with nominal adverse impact on use of the Service or on Client’s key business processes	within 2 business days

Client’s sole and exclusive remedy for Kyndryl’s failure to meet the response time will be a $750 credit for each failed Severity 1 response, $500 for each failed Severity 2 response, and $250 for each failed Severity 3 response.

SLA-4. Resolution Time SLA

Resolution of the problem ticket will be based on the criteria listed below:

Label	Definition	Resolution Time
Severity 1	Incident that prevents all Client use of the Service	Less than 5 hours

Resolution Time – is measured from time the service Incident report is received at Kyndryl Service Desk to point in time when the Incident is resolved, or workaround is in place and the Kyndryl support personnel submits the resolved service Incident notice to Client for confirmation of resolution.

In the event of Go-Live of new functionality, an Upgrade, or significant change in the Architecture of the Application Environment, this service level will be suspended temporarily subject to the applicable stabilization period.

P-1. Pricing

Rates and charges for Application Management for Oracle on Any Cloud are found in the applicable section of this Service Guide or in the applicable Schedule.

A-1 Security Roles & Responsibilities

The following table lists security responsibilities and states which party is responsible for each one by inserting an “R” in the appropriate column for Kyndryl or Client.

Category	Task	Kyndryl	Client
Information Security Policies	Perform periodic systematic identification and evaluation of risks pertaining to the scope of the Agreement.	R	R
Information Security Policies	Perform risk and regulatory reviews and determine appropriate base security controls.	R	R
Information Security Policies	Maintain Security Document and exception process.	R	
Information Security Policies	Evaluate exception requests posing risk to the larger Kyndryl business and other Clients.	R	R
Information Security Policies	Evaluate base controls in the Kyndryl-managed portion of their environment to address requirements created by business strategy, regulations, legislation and contracts, and the current and projected information security threat environment.		R
Information Security Policies	Communicate to Kyndryl their need for more stringent controls or risk acceptance of less stringent controls.		R
Information Security Policies	Notify Kyndryl of all applicable regulatory requirements and inventory of affected devices.		R
Information Security Policies	Comply with its obligations as Data Controller and inform Kyndryl of any additional data processing requirements relating to the Kyndryl services subject to this document.		R
Information Security Policies	Notify Kyndryl of changes to processing, security or regulatory requirements.		R
Information Security Policies	Remain in compliance with the Security Document including regulatory requirements and approved exceptions.		R
Information Security Policies	Provide Maintenance windows and support resources to maintain compliance.		R
Organization of Information Security	Provide a focal point for protection of its information assets and coordination of security related activities.		R
Organization of Information Security	Provide contact method for a primary and secondary security focal.	R	R

Category	Task	Kyndryl	Client
Organization of Information Security	Interface with the Client regarding the security document and its implementation per the Agreement.	R	
Organization of Information Security	Provide a schedule of maintenance windows.	R	R
Organization of Information Security	When Client signs IaaS contract with IaaS Provider directly, Client adds “aaS” Oracle as subprocessor in their DPA exhibit.		R
Organization of Information Security	When Client signs IaaS contract with IaaS Provider directly, Client provides Kyndryl with a copy of their DPA Exhibit as evidence the “aaS” is captured as a subprocessor.		R
Human Resource Security	Address security requirements in the hiring, termination and personnel management processes for personnel they manage.	R	R
Human Resource Security	Provide security awareness training to personnel they manage.	R	R
Human Resource Security	Take appropriate management action if there is a misuse of authority by personnel they manage.	R	R
Asset Management	Identify and communicate Client data or information requiring special handling.		R
Asset Management	Arrange with IaaS provider to provide data removal meeting NIST-800-88 or other regulatory requirements for residual Client data after storage is deallocated by Kyndryl.		R
Asset Management	Manage information identified by the Client as confidential information per Security Document.	R	
Cryptography	Define and provide to Kyndryl Client’s data protection and handling requirements, if different from Security Document.		R
Cryptography	Provide and support encryption contained in the respective components they manage.	R	R
Cryptography	Generate, distribute and manage data encryption keys for the respective components they manage.	R	R
System Acquisition, Development and Maintenance	Implement Security Document controls in systems acquisition and activation for Kyndryl-managed components.	R	
Supplier Relationships	Establish contracts/agreements with external suppliers they manage.	R	R
Supplier Relationships	Coordinate all security activities with third parties managed by their organization.	R	R
Supplier Relationships	Establish policies and procedures for external suppliers they manage with access to information within their scope.	R	R

Category	Task	Kyndryl	Client
Supplier Relationships	Monitor performance against contracts/agreements/policies with external suppliers they manage.	R	R
Security Incident Management	Promptly report any security issues in the Kyndryl managed environment.	R	R
Security Incident Management	At their discretion, arrange for Kyndryl Incident Response and Intelligence Services (IRIS) or a comparable service. Managed Apps does not provide comprehensive incident response or forensic services. .		R
Security Incident Management	Cooperate in initial security incident evaluation.	R	R
Security Incident Management	Take actions to resolve security incidents involving networks, systems, data and personnel managed.	R	R
Security Incident Management	Interface, as needed, with external entities such as law enforcement, legal or regulatory agencies.	R	R
Security Incident Management	Responsible for the business continuity including assessment, planning, testing and maintenance. Business continuity planning should include information security.		R
Operations Security	Provide a security audit focal point to coordinate IT audit support activities.	R	R
Operations Security	Provide support for IT audit activities such as data collection, audit tool installation and report generation.	R	R
Access Controls	Authorize user ids and privileges for components they manage.	R	R
Access Controls	Administer passwords on components they manage.	R	R
Access Controls	Reset and disclose passwords for components they manage.	R	R
Access Controls	Perform Employment Verification for their personnel on components they manage.	R	R
Access Controls	Perform Business Need Revalidation for their personnel on components they manage.	R	R
Access Controls	Configure a Business Use Notice for components they manage.	R	R
Access Controls	Identify and implement the protection and access logging requirements for user resources in components they manage.	R	R
Access Controls	Implement the functions and features of the software to set initial access controls for new folders, directories or files, for software components they manage.	R	R

Category	Task	Kyndryl	Client
Access Controls	Identify the protection requirements for critical system and software product files for software they manage.	R	R
Access Controls	Manage changes to components they manage according to the Change Control Process.	R	R
Access Controls	Maintain compliance in the installation, maintenance and upgrades of software components they manage.	R	R
Access Controls	Capture and manage access records for components they manage, per the Security Document.	R	R
Operations Security – Network	Capture and manage logging functions for network components managed.	R	R
Communications Security	Manage the internal and Internet-facing network infrastructure security for segments managed.	R	R
Communications Security	Manage network security infrastructure components they manage, used for the inter-connection of Client network and Kyndryl network.	R	R
Communications Security	Establish procedures for logging, alarming and reporting of network security violations on network devices they manage.	R	R
Communications Security	Perform periodic configuration reviews on Kyndryl managed network infrastructure components.	R	
Communications Security	Manage access to Kyndryl-managed software that monitors, manages, manipulates or modifies network configurations and traffic on infrastructure network segments managed by Kyndryl.	R	
Communications Security	Implement and manage in-scope intrusion-detection and/or intrusion-prevention components on infrastructure network segments managed by Kyndryl.	R	
Compliance	Define policies and standards for Health checks and vulnerability scanning.	R	
Compliance	Perform vulnerability scans on Kyndryl managed firewalls (excluding IaaS managed firewalls) and at VM, OS and DB hosted platform level for all Client systems.	R	
Compliance	Provide summary results of vulnerability scans upon request.	R	
Compliance	Take timely corrective action to address vulnerabilities, in accordance with risk level.	R	R
Compliance	Notify Client if vulnerabilities require Client's immediate attention.	R	

Category	Task	Kyndryl	Client
Compliance	For Client managed components, take timely corrective action to address vulnerabilities requiring immediate attention.		R
Operations Security – Compute	Provide and operate malware detection software for systems under Kyndryl management.	R	
Operations Security – Compute	Respond to malware incidents on systems and devices they manage.	R	R
Operations Security – Compute	Implement real-time scanning for malicious code on managed end points.	R	
Operations Security – Compute	Perform automated system security health assessment and enforcement for software managed by Kyndryl.	R	
Operations Security - Software Maintenance (systems, network, storage)	Communicate planned security patch and update maintenance windows for Kyndryl-managed software components.	R	
Operations Security - Software Maintenance (systems, network, storage)	Provide automation to support unattended installation of security patches and upgrades (e.g., automated application shutdown/restart).		R
Operations Security - Software Maintenance (systems, network, storage)	Assemble, and test patch bundles for Kyndryl-managed software components and notify Client of contents.	R	
Operations Security - Software Maintenance (systems, network, storage)	Install patch bundles in scheduled maintenance windows for all Kyndryl-managed software components and notify Client of results.	R	
Operations Security - Software Maintenance (systems, network, storage)	Provide for testing if required for approval prior to deploying patches and updates.		R
Operations Security - Software Maintenance (systems, network, storage)	Responsible for the management and installation of security patches and updates for all software components not managed by Kyndryl.		R

Category	Task	Kyndryl	Client
Operations Security - Software Maintenance (systems, network, storage)	Maintain awareness of available security patches and upgrades for their environment, assess their applicability and determine their urgency.		R
Operations Security - Software Maintenance (systems, network, storage)	Notify Kyndryl promptly when installation of security updates is required prior to the next scheduled maintenance window.		R
Operations Security - Software Maintenance (systems, network, storage)	Communicate impacts of anticipated and currently unsupported software components managed by Kyndryl.	R	
Operations Security - Storage	Perform back-up and restore of storage assigned to the Client per Agreement.	R	
Operations Security - Storage	Responsible for data removal meeting NIST-800-88 or other regulatory requirements.		R
Operations Security - Storage	Notify Kyndryl promptly when installation of Storage security updates is required prior to the next scheduled window.		R
Operations Security - Storage	Client must provide for testing if required for approval to deploy updates.		R
Operations Security - Storage	Communicate impacts of anticipated and currently unsupported Storage components.	R	

A-2 Supported Software

Kyndryl supports software as listed below.

For use of BYOL application and database software (BYOL Software) managed by Kyndryl in the Managed Service, Client must have properly acquired authorizations and sufficient license entitlement from the licensor of such software (Entitlements). Client is responsible for auditing their licenses and ensuring that they have sufficient license entitlements.

If Client is found to be using a software version no longer maintained or supported by the manufacturer (for Oracle products - those no longer under Mainstream or Extended Maintenance or not under a valid Oracle support contract), Kyndryl is excluded from responsibility for failure to meet the expected Service Level for any Service Level Default due to such use of unmaintained software by the manufacturer, and Kyndryl will only be responsible to provide support on a reasonable efforts basis. Version upgrades or updates necessary to maintain any supported software require the Client to execute an Order Document with Kyndryl at additional cost.

Oracle Products

Kyndryl provides managed service for Bring Your Own Licenses (BYOL) Oracle applications and releases where the Oracle application/Oracle component/OS/DB combination is stated in the Oracle Product Certification Matrix and the OS/DB combination is listed as supported.

The following is partial list of the currently supported BYOL Oracle applications software. Kyndryl will provide a full list upon request.

BYOL Oracle Application Software		
Oracle eBusiness Suite	PeopleSoft	JD Edwards
Oracle Retail Applications (Retek)	Primavera	Demantra
Oracle Enterprise Manager	EPM/Hyperion	Oracle Financial Services (Oracle FLEXCUBE Core Banking)
Oracle Fusion Middleware	Agile	Advanced Supply Chain Planning
Oracle Business Intelligence Enterprise Edition – OBIEE	Oracle Golden Gate	Oracle GRC
Oracle GTM	Oracle MFT	Oracle Single Sign-On
Oracle Transportation Management (OTM)	Oracle UPK	Oracle Value Chain Planning (VCP)

Oracle Add-Ons

If selected by Client, the following Add-ons will be integrated with the Oracle Application at additional charges:

BYOL Software Add-ons		
Vertex	Sabrix	Taxware
Quest STAT	APEX	IBM WebSphere

Middleware Products

Based on the OS/DB Release combinations above, Kyndryl will provide Managed Services for middleware software products at different charges for the following middleware-components and charge types as listed below:

Middleware Products		
Dev Tools (Windows Development Tools Platform)	Oracle Application Integration Architecture Foundation Pack	Oracle Data Integrator
Oracle Enterprise Repository	Oracle Identity and Access Management	Oracle Identity Management
Oracle Service Bus	Oracle SOA Governance (Oracle Enterprise Repository, Oracle Service Registry)	Oracle SOA Suite and Oracle Business Process Management Suite
Oracle SOA Suite Components	Oracle WebCenter Content	Oracle WebLogic Server

A-3. Definitions

The definitions below apply to all Kyndryl Services for Oracle Applications Management for multiple cloud environments. Additional definitions may be provided in the applicable Schedule.

APIs – application programming interfaces Kyndryl provides as Service Component which provide programming code to interface with and utilize the Services, including requesting and ordering Services options and Service Components, which bypass Cloud Web Portal user interfaces.

Availability – means a Client end-user's ability to access the production environment over the Infrastructure. Availability is calculated in accordance with the following formula: x = [(n - y) * 100]/n, where x = Availability percentage, n = total hours per month, and y = hours the Service was not available solely because of an act or omission by Kyndryl for Services within Kyndryl's direct control as detailed in applicable Parts of the Schedule (excluding Maintenance).

Application – means the Oracle service component software that is to be managed by Kyndryl and listed in the Usage Entitlements section of the Pricing Configuration/Charges Schedule.

Application Environment – means the configuration of services components and content which result in the deployment of definable instances of the Application that serve a distinct business purpose, such as development, testing, training, demonstration or production use.

Change Request – modifications requested by Client and undertaken by Kyndryl to the Client environment submitted via Kyndryl's Change Request management process for risk and planning consideration.

Client or Client Agent – the Enterprise company identified in the signature block of the Order Document that incorporates services from this Service Guide and its Users.

Cloud IaaS Provider – a data center facility where Kyndryl provides the Services from and where Services Components are hosted and made available for Client use via Client owned account. IaaS provider provides equipment and software applications provided and managed by Kyndryl and the Client that constitutes the physical and virtual computing, storage and network devices used to run software operating systems and applications, and may also include, but is not limited to, routers, switches, servers, and peripheral devices (including security service devices and fiber optic), used to provide the Service.

Content – Content consists of all data, software, and information that Client or its authorized users provides, authorized access to, or inputs to Services.

Contract Month – means each calendar month during the initial Term and any Renewal Term commencing with the first full month after the Go Live Date.

Kyndryl – Kyndryl, Inc or its Enterprise (or offshore company operating in Client's country) that makes the Services available for the country specified in the Client's business address provided upon acceptance of this Service Guide.

Image – a software image file containing the functionality of the software program(s) that Kyndryl makes available as part of the Services. An Image contains an Operating System Image by itself or in conjunction with a Kyndryl Image or Third-Party Image.

Incident – means an unplanned IT service disruption affecting normal operations to any of Client's Services provided under a Schedule.

Internet – the public worldwide network of IP-based networks.

Go-Live or **Go-Live Date** – means the date when the different Application Environments will be used for their distinct productive business purpose by the Client e.g., development or production. After initial Go-Live the introduction of new Application functionality, an Upgrade, or significant change in the architecture of the Application Environment will result in additional Go-Live Dates during the contract duration.

Non-Production Application Environment – means the specific Application Environment is not used for "production" and may be used for other purposes such as development, testing or training. Non-Production Application Environment instances that require additional or dedicated hardware may require additional charges. Client acknowledges that in the event of an Application problem or Update, Kyndryl may utilize Client's test designated Non-Production Application Environment for troubleshooting or other testing required to resolve the problem or test and apply the Update as applicable. During such time Kyndryl will have priority use of the Non-Production Application Environment.

OS – Operating System software.

Order and Pricing Schedule (or Schedule) – means an ordering document signed by Kyndryl and Client that is required for Client’s initial order and any additional orders.

Portal – Kyndryl Web site(s) designed to enable Client to use the Services and view additional Services options and Account information.

Production Application Environment – means the specific environment intended for use by Client, or its authorized third parties, as it utilizes the Application in support of its ongoing business operations.

Responsibility Matrix – means the tasks which are designated as Kyndryl or Client are responsible to complete.

Service Level – means the service level of assigned as the target for an SLA.

Service Level Default – means Kyndryl's failure over the course of a Contract Month to achieve the expected Service Level.

Service Component Software – software functionality that Kyndryl makes available as a Service Component.

Service Activation Date – a date when Kyndryl notifies Client that Kyndryl Services are available for Client use. Services may be initiated in stages (for example per each environment) and charges will begin for any portion of Services being received by Client as of each Service Activation Date.

Service Components – the hardware, software, Service Component Software, APIs, tools, and any documentation (electronic or otherwise) Kyndryl utilizes to provide the infrastructure, Cloud Web Portal, and functionality of the Services or that Kyndryl makes available as part of the Services.

Service Plan – 10 Change Requests or Service Requests per calendar month as requested by Client.

Service Request – means any request for Services or information made by Client to Kyndryl in accordance with Kyndryl’s Service Request management process.

Service Tier – predetermined Client experience specified by Kyndryl for servicing and managing Kyndryl and Client relationship.

Services Credit – an amount equal to ten percent (10%) of Client's current monthly recurring charges one (1) of the affected systems only (excluding any applicable taxes and fees).

Solution – Client-created software application service solution Client makes available to Solution Recipients in a VM.

Solution Recipients – means any entities or individuals to whom Client provides access to a VM or product or services that Client offers in a VM.

Usage Entitlements or **Entitlements** – mean the Authorizations and business parameters relating to Client's use of the Services that are set forth in the Charges Schedule and are used in part to determine the fees paid by Client for the Services (e.g., users, transactions, storage).

VM – a virtual machine instance that Kyndryl makes available to Client as part of the Services consisting of virtual computer processing unit(s) ("CPUs"), virtual memory and virtual local storage.

End of Service Guide

This document is current as of the initial date of publication and may be changed by Kyndryl at any time.

Not all offerings are available in every country in which Kyndryl operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NONINFRINGEMENT.