



Microsoft Dynamics 365 for
Finance and Operations

Service description

*Version 8
July 2018*

Overview	03
Operating model	05
System configuration	08
Service operations	10
Onboarding and implementation	11
Tenant and data management	12
Data back-up and retention	14
Service activity responsibilities	14
Service update strategy and maintenance windows	16
<i>Planned maintenance responsibilities</i>	17
<i>Microsoft planned maintenance schedule and communication</i>	20
Security and administrative access	20
Monitoring and incident management	21
<i>Monitoring</i>	21
<i>Incident management</i>	22
Business continuity with high availability and disaster recovery	23
Application support offerings	24
<i>Process to engage support</i>	24
Service Level Agreement (SLA)	24
Library	25
Definitions	27



Overview

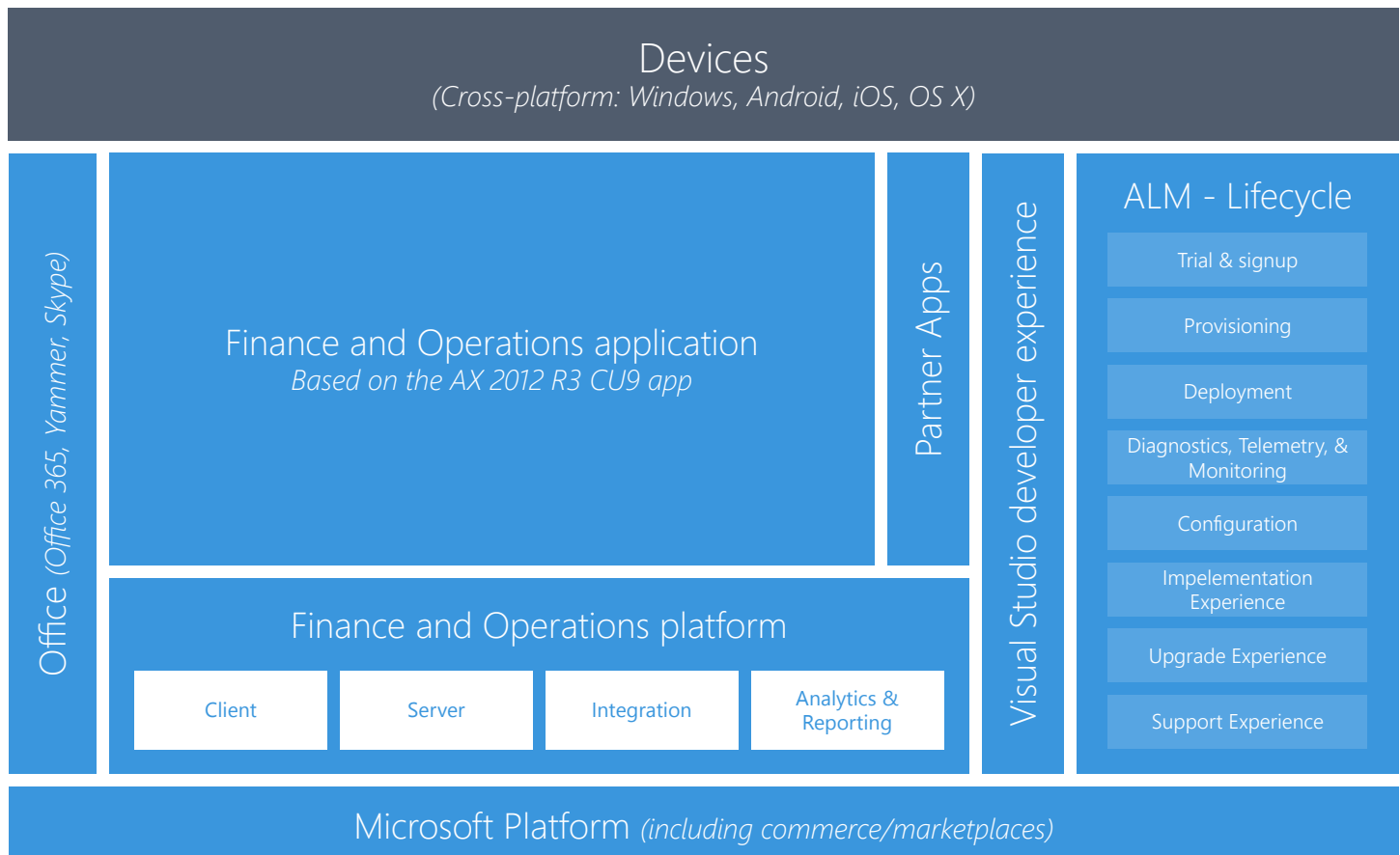
Overview

Overview

Microsoft Dynamics 365 for Finance and Operations ("Finance and Operations") is a cloud Enterprise Resource Planning (ERP) service for enterprises, built on and for Microsoft Azure. It provides organizations with ERP functionality that supports their unique requirements and helps them adjust to constantly changing business environments, without the hassle of managing infrastructure. Finance and Operations brings together a set of ERP, business intelligence, infrastructure, compute, and database services in a single offering that enables organizations to run industry-specific and operational business processes that are extendable with specific solutions from Independent Software Vendor (ISV) (see Microsoft AppSource). Organizations can match their business growth by easily adding users and business processes with a simple, transparent subscription model (more information: [here](#)).

The Finance and Operations cloud service is composed of the components illustrated in **Figure 1**.

Figure 1: Overview of the Finance and Operations cloud service



Click buttons for more info.

[Microsoft AppSource](#)

[Licensing Guide](#)



Operating model

Operating model

Operating model

The operating model of Finance and Operations distinguishes specific roles and responsibilities for Customer, Implementation Partner, and Microsoft throughout the lifecycle of the service as illustrated in **Figure 2**.

Microsoft maintains the Finance and Operations service by deploying, actively monitoring, and servicing the Customer's production tenants. This includes allocating the required system infrastructure to run the service and proactive communication to Customers about the service's health.

Support provided by Microsoft

Infrastructure

- Storage and database capacity management
- High availability and disaster recovery
- Platform security
- Infrastructure capacity, scale up and down
- Infrastructure management and deployment
- Data center networking, Power & Cooling



Application platform

- Diagnostics, patches, updates, hotfixes, and updates
 - Network management
- App monitoring and first line support

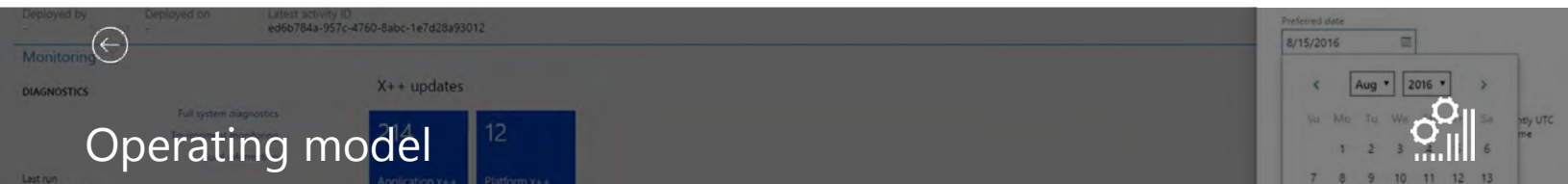
User/data

- Security, identity configuration, and management

Application

- Define and test business processes
- Develop and test customizations
- Monitoring of sandbox environments

Customer leading, supported by Implementation Partner



Operating model

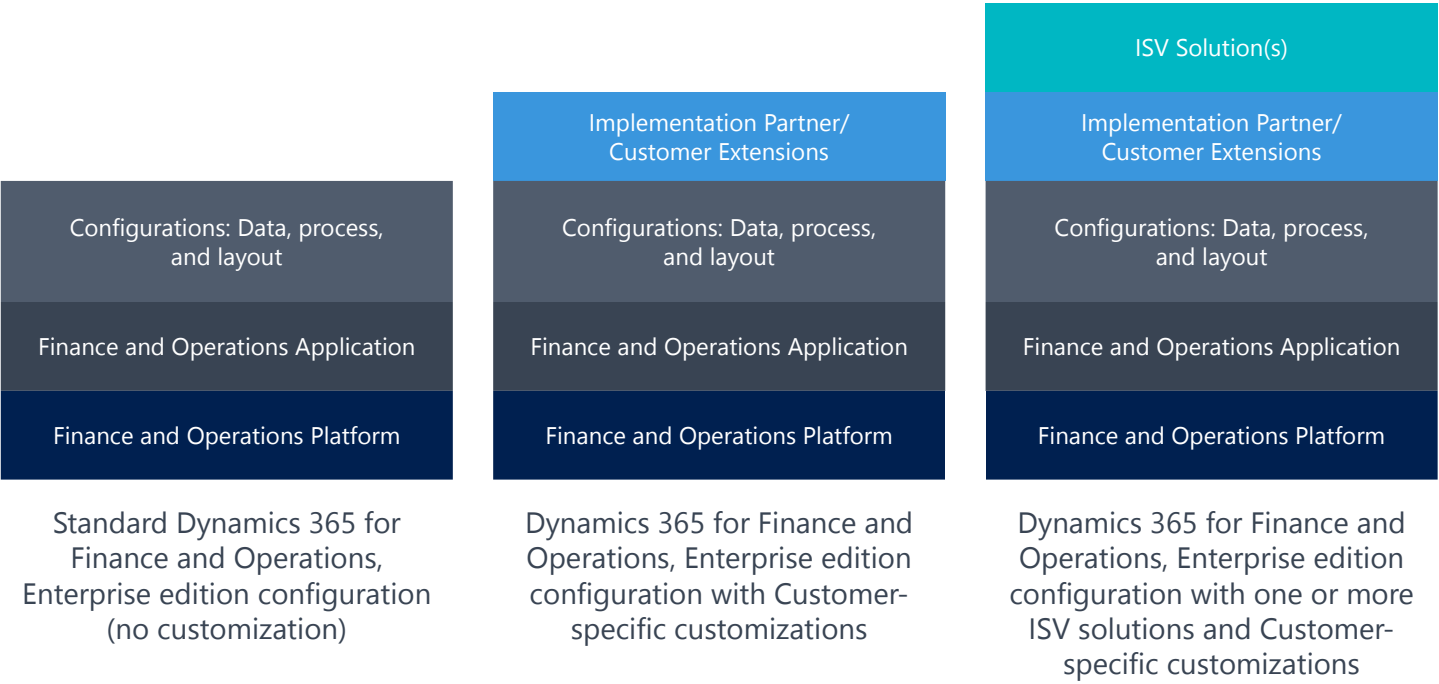
With the support of their Implementation Partner, Customers determine the configuration of the business application logic in Finance and Operations to match their unique business processes. Customers can extend Finance and Operations with ISV solutions of their choice, unique customizations, or a combination of these. Customers typically choose one of the following configuration scenarios (also shown in **Figure 3**):

7

- **Solution 1:** Standard Finance and Operations configuration (no customization)
- **Solution 2:** Finance and Operations configuration with Customer-specific customizations
- **Solution 3:** Finance and Operations configuration with one or more ISV solutions and Customer-specific customizations

For any of these scenarios, the Customer defines, develops, and tests any modifications using Microsoft Dynamics Lifecycle Services (LCS) and tools.

Figure 3: Common configuration scenarios





System configuration

The banner features a dark background with four bar charts. The first chart on the left has a circular arrow icon above it. The second chart has a gear icon above it. The third chart has a bar chart icon above it. The fourth chart on the right has a gear icon above it. The text 'System configuration' is overlaid on the first chart.

System configuration

System configuration

Finance and Operations scales with transaction volume and User load. Each Customer implementation of Finance and Operations produces a unique solution due to the following variables:

- **Data composition:** A unique set of parameters that control behavior, layout of the organization, structure of master data (such as financial and inventory dimensions), and granularity of transaction tracking.
- **Customization and configuration:** Extension mechanisms of Finance and Operations with code customizations, ISV solutions, and unique configurations including workflows, integrations, and report configurations.
- **Usage patterns:** A unique combination of online and batch usage combined with the ability to integrate with upstream and downstream systems for unified data flow and the ability to differentiate based on the information views used by Customers in their business processes.

Microsoft configures production tenants sized to handle the transaction volumes and user concurrency. Microsoft is responsible for:

- Proper allocation of resources of production tenants, based on the Customer's profiling information in the LCS Subscription Estimator
- Continually monitoring and diagnosing service availability of production tenants
- Analyzing and troubleshooting system performance issues with Finance and Operations

To ensure that a particular implementation is configured for high performance, Customers must:

- Provide accurate usage information for the Finance and Operations implementation through the LCS Subscription Estimator
- Build and test customizations for performance and scale
- Test data configurations appropriately for performance



Service operations

1. Onboarding and implementation
2. Tenant and data management
3. Data back-up and retention
4. Service activity responsibilities
5. Service update strategy and maintenance windows
6. Security and administrative access
7. Monitoring and incident management
8. Business continuity with high availability and disaster recovery
9. Application support offerings
10. Service Level Agreement (SLA)



Service Operations

Service operations reflect various aspects of provisioning and use of Finance and Operations, from onboarding and implementation to updates and monitoring and through service termination. For each successful implementation of Finance and Operations, Microsoft, the Customer, and Implementation Partners or ISVs (when applicable) have specific roles and responsibilities.

11

- 1 Onboarding & implementation
- 2 Tenant & data management
- 3 Data back-up & retention
- 4 Service activity responsibilities
- 5 Service update strategy & maintenance windows
- 6 Security & administrative access
- 7 Monitoring & incident management
- 8 Business continuity with high availability & disaster recovery
- 9 Application support offerings

Onboarding and implementation

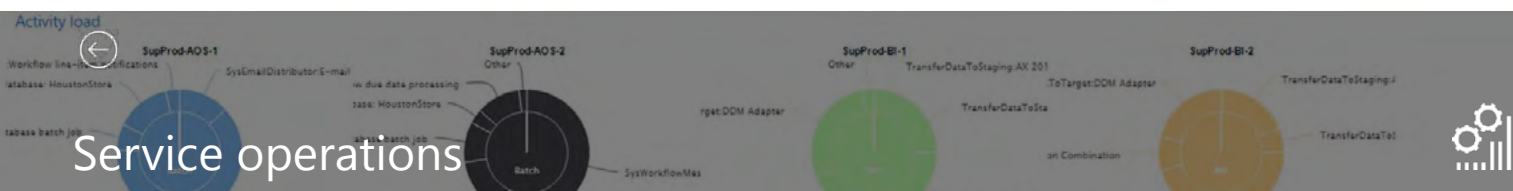
Typical onboarding and implementation events and the expected responsibilities for each party are provided in **Table 1**.

Table 1. Onboarding and implementation events

Request	Expected Microsoft action	Expected Customer/ Implementation Partner action
Initial offer purchase	LCS project is created after the purchase of the offer.	Go through EA or CSP onboarding process. Partner creates tenant for Customer, if applicable.
Add-On purchase	Grant Customer access to Add-On selected during the implementation.	Not applicable.
Implementation planning and analysis	Provide relevant tools in LCS, such as Business Process Modeler and interoperability with Visual Studio Online.	Project planning, Visual Studio Team Services, System onboarding and admin account setup.

More information about the onboarding process is published here (login required).

More info



Tenant and data management

Typical tenant and data management events for any Service and the responsibilities for each party are described in **Table 2.1** for Production Instances and **Table 2.2** for Non-Production Instances. Customer's requests must be submitted to Microsoft using the Service Request in LCS.

12

Table 2.1. Tenant and data management events for Production Instance

Customer's request	Customer's responsibility	Microsoft's responsibility	Microsoft's lead time	Microsoft's estimated maintenance downtime
Deploy a new Production Instance	<ul style="list-style-type: none"> Accurately complete the sizing questionnaire in the LCS Subscription Estimator before requesting a Production Instance. Complete all implementation tasks specified in the LCS checklists. 	<ul style="list-style-type: none"> Complete Go live health check from Microsoft Fasttrack Services. Deploy a Production Instance only after Customer has completed all LCS checklists and notify Customer of the provisioned environment through email. 	2 business days	N/A
Copy a Non-Production Instance database to a Production Instance before go-live (Note: This request is not available if Customer already is live in production)	Validation and sign-off.	Copy a Non-Production Instance (e.g., Sandbox Tier2 Add-on) database to a Production Instance as part of the go-live process.	5 hours	1-4 hours
Maintenance mode	Complete necessary maintenance. Request to put the AOS back into active mode.	Put AOS in maintenance mode	5 hours	2 hours

Service operations

Microsoft will provide point in time restoration of Customer's Non-Production Instance databases as described in **Table 2.2**.

Table 2.2. Tenant and data management events for Non-Production Instances

Customer's request	Customer's responsibility	Microsoft's responsibility	Microsoft's lead time	Microsoft's estimated maintenance downtime
<i>New sandbox instance</i>	<ul style="list-style-type: none"> Ensure all the instances needed, have been planned and Add-On offers purchased. Complete all implementation tasks specified in the LCS checklists. 	<ul style="list-style-type: none"> Ensure instance request is against a base subscription or an Add-On offer. Deploy the instance and notify the Customer and Implementation Partner. A sandbox instance is a Tier-1 development or build environment or a Tier-2 (or higher). Tier-2 (or higher) environment are multi-box environments closer in topology to a production environment. 	2 business days	N/A
<i>Copy golden configuration database from Dev/Test to Sandbox before go-live</i>	<ul style="list-style-type: none"> Validation and sign-off. Prepare and export the database from a development environment (Tier 1). Import and update the database to a sandbox environment (Tier 2 or higher). 	N/A	N/A	1-4 hours
<i>Copy a Production Instance database to a Non-Production Instance</i>	<ul style="list-style-type: none"> Post-copy: Delete or obfuscate sensitive data, adjust environment specific application configuration (such as integration endpoints) and enable or add users. Customer should make these changes by applying a data package. 	<ul style="list-style-type: none"> Copy Production Instance database to the Non-Production Instance Customer specifies. Restrict user access to Admin user only. Withhold batch jobs, remove SMTP email and printing configuration on the Non-Production Instance database 	5 hours	1-4 hours
<i>Non-Production Instance database point in time restore</i>	<ul style="list-style-type: none"> Accept that process cannot be undone. 	<ul style="list-style-type: none"> Restore a Non-Production Instance database (Tier-2 or any Tier Add-on) to a point in time in the past. 	5 hours	1-8 hours
<i>Copy Tier 2 Sandbox database to a Tier 1 Sandbox for troubleshooting and debugging</i>	<ul style="list-style-type: none"> Copy, repare and export the database from sandbox environment. Import and update the database in Tier 1 environment 	N/A	N/A	1-4 hours

These data management activities will be made self-service through LCS in the coming months.



Data back-up and retention

Databases are protected by automatic back-ups. Automatic back-ups are retained for 35 days unless Microsoft performs a rollback. Rollbacks may be performed in the event a failure occurs during any planned maintenance update specified in **Table 4**.

Databases are protected by automatic back-ups as described here.

Automatic back-ups

14

Service activity responsibilities

Table 3 describes some typical scenarios and activities for each Service along with the responsibilities of Microsoft, Customer, or both concerning such activities..

Table 3. Activities managed by Microsoft of Customer

	Responsible party	
Activity	Microsoft	Customer
Provisioning initial tenants		
Size projected load in LCS using the Subscription Estimator tool and request specific environment(s) to be provisioned		●
Provision all Production Instances and Non-Production Instances	●	
Validate the deployed Production Instances and Non-Production Instances		●

Application updates

(Hotfixes, patches, updates, integrations, and customizations)

Download update from LCS and define, develop, test the update, and provide code update package back to LCS		●
Request updates to be applied to the Production Instance		●
Create code and data backup for Production Instance before applying any updates	●	
Apply code update to Production Instance	●	
In case of any failure, roll back Production instance to code and data backup	●	

Data management (Backup, restore, and update)

Backup database	●	
Determine HA and disaster recovery plan	●	
Monitor Production Instance database performance.	●	●
Tuning the Production Instance database for performance.	●	●
Initiate copy of Production Instance database to Non-Production Instance		●

- applicable to the designated party



Activity	Responsible party	
	Microsoft	Customer
Update infrastructure		
Execute scheduled updates to the infrastructure updates	●	

Scale up and down (Users, storage, instances)		
Purchase additional users and non-production add-ons		●
Changes in usage must be updated in the LCS' Subscription Estimator tool		●
Report any significant performance issues impacting usage of the applicable Service		●
Proactively manage the resources needed for the applicable Service	●	
Investigate and troubleshoot Incidents	●	●

Security (User access)		
Provide user access to the applicable Service		●
Provide LCS project access for managing and operations instances deployed through LCS		●

Monitor Production Instance		
Monitor Production Instances 24x7	●	●
Notify Customer proactively of Incidents with the Production Instance	●	

Manage and Monitor Non-Production Instances		
Manage Non-Production Instances with LCS		●
Monitor Non-Production Instances		●

● applicable to the designated party



Service update strategy and maintenance windows

Customer must stay current on all platform updates and application updates for Finance and Operations pursuant to the software lifecycle policy. All versions of Finance and Operations will use the new Microsoft Modern Lifecycle Policy. The Modern Lifecycle covers products that are serviced and supported continuously.

The updates to Finance and Operations application and platform are handled as follows.

- **Platform Updates** are updates to the Finance and Operations platform. Microsoft notifies customers when they release an update to the platform. Microsoft requires each Customer to be current on the latest Finance and Operations platform update. Starting April 2018, Microsoft will update your environments to the latest release of the platform within the planned maintenance schedule specified in Table 5. Customers can also get the update via LCS and can apply the update to their environments on their own prior to Microsoft initiating the update.
- **Application Updates** are updates to the Finance and Operations application. These updates are optional. A Customer indicates acceptance of updates by providing consent, after which the application updates are applied by Microsoft to the Customer's production environment.

Updates are provided as X++ code or a binary (deployable package). X++ updates must be applied on a development environment before they can be deployed on a sandbox, staging, or production environment. Binary updates can be applied directly on any environment, but must be validated on the Customer's sandbox environment before being promoted to a production environment. Refer to Table 4 for more detailed instructions.

Some updates may be mandatory and require no consent. To help protect our Customers and the service, Microsoft may apply critical security updates directly to a Customer's Finance and Operations production environment.

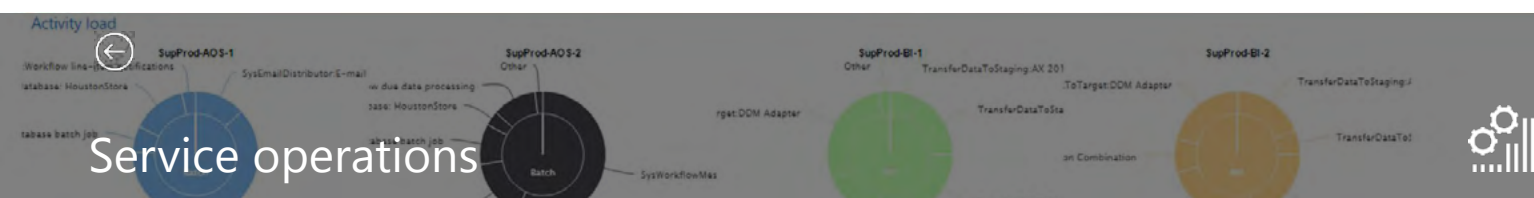
Software lifecycle policy.

Policy

16

For more information see the Finance and Operations update policy.

Update policy



Planned maintenance responsibilities

Microsoft provides Customers with the types of updates to the Finance and Operations service set forth in **Table 4**. These updates may require down-time on the production environment. The downtime window can be categorized as Microsoft Planned Maintenance (initiated by Microsoft) or Customer Planned Maintenance (initiated by the Customer). Updates are scheduled with the Customer via LCS.

17

The responsibilities of Microsoft, the Implementation Partner, and the Customer are reflected in **Table 4** for each update type.

Table 4. *Planned maintenance for updates*

Type of update Description	Expected action		Maintenance window Microsoft's estimated maintenance downtime
	Microsoft	Customer/ Implementation Partner	
Platform			
Hotfix <i>Fix for a specific issue that the Customer reported, Microsoft may relase a fix on the latest latest platform.</i> <i>Platform updates, released as a deployable package, will be cumulative and replace existing binaries.</i>	Publish platform updates to LCS.	Apply on all Non-Production Instances (including Sandbox Tier 1: Developer Instance); validate and sign-off; and then promote to Production Environment	Customer initiated maintenance window <i>30 minutes - 4 hours*</i>
Critical security updates <i>Update that addresses a critical security vulnerability.</i>	Initiate critical security updates within the Microsoft planned maintenance window.	No action needed.	Microsoft initiated maintenance window <i>30 minutes - 4 hours*</i>
Platform rollups (Platform updates) <i>Platform updates are collections of hot fixes and new features for the platform, provided as a deployable package. They are backward compatible.They are also backwards compatible with the last major release of the applicable Service.</i>	Initiate updates to the platform within the Microsoft planned maintenance window.	Customer must always stay current on the latest version of the platform.	Microsoft initiated maintenance window <i>30 minutes - 4 hours*</i>

Continued on next page



Type of update Description	Expected action		Maintenance window Microsoft's estimated maintenance downtime
	Microsoft	Customer/ Implementation Partner	
Application			
Hofix/Monthly update <i>Fix for a specific issue that the Customer reported or Microsoft discovered in the application or new features. Hotfixes are delivered in one of two formats: X++ or binary.</i>	Publish the update in LCS.	Binary: Apply on any Non-Production Instance; validate; and then promote to ProductionInstance. X++: Apply on dev environment; test; deploy on designated Non-Production Instance; validate; and then promote to Production Instance.	Customer initiated maintenance window <i>30 minutes - 4 hours</i>
Critical update <i>Update that solves a critical issue.</i>	Notify Customer of the critical update. Initiate update within the specified timeline.	Apply the critical update.	Customer initiated maintenance window <i>30 minutes - 4 hours</i>
Major releases <i>Major releases for the applicable Service include new functionality.</i>	Make the new major release available and publish to LCS.	Prepare for the upgrade according to the LCS instructions and best practices.	Customer initiated maintenance window <i>5 - 8 hours</i>
Customizations <i>Change to the standard business application logic.</i>	No action required.	Validate customizations in Customer's Non-Production Instances and then promote them to Customer's Production Instance.	Customer initiated maintenance window <i>1 - 4 hours</i>

Continued on next page



*Promoting an update to a Customer's production environment is a service request to Microsoft that must be initiated from LCS. This is within the Customer planned maintenance window. Request is planned to be executed within two business days. Generally, 95% of updates are applied in less than an hour. (N/A means not applicable.)



Microsoft planned maintenance schedule and communication

Scheduled downtime means periods of downtime² related to network, hardware, or Service maintenance or upgrades. Microsoft will publish notice or notify Customers at least **five days** prior to the commencement of such downtime. The default downtime window as listed below are scheduled on weekends in time windows defined per region to minimize the impact to the Customers' business.

Downtime has the meaning given to it in the SLA.

20

Microsoft's Planned Maintenance Schedule.

- **NAM:** 2 AM - 10 AM
- **SAM:** 12 AM - 8 AM
- **EMEA:** 10 PM - 6 AM
- **CAN:** 2 AM - 10 AM
- **APAC:** 12 PM - 9 PM

Security and administrative access

Administrative access to a Finance and Operations production environment is strictly controlled and logged. Customer Data is handled in accordance with the Microsoft Online Services Terms. Customer's tenant administrator can access Production Instances or Non-Production Instances as described in **Table 5**. Microsoft's Administrator access is described in **Table 5**.

Microsoft Online Services
Terms.

Online Services Terms

Table 5. Customer's administrative access

Environment type	Purpose	Level of Customer access
Non-Production Instance - Sandbox Tier 1: Developer Instance	Non-production instance that Customer can use for development or as build machines or to customize any Service and unit test Customer changes.	As of platform update 12 for the applicable Service, Customer will not have administrator access to development environment VMs running in the Microsoft subscription. Customer will continue to have full administrative access to the SQL Azure server installed on the environment.
Non-Production Instance – Sandbox Tier 2: Standard Acceptance Testing Instance (or any Sandbox Tier Add-on)	Non-production instance that Customer can use for user acceptance testing, integration testing, and training of any Service.	Customer will not have remote desktop access or access to the SQL server associated with the Non-Production Instance. Customer can connect as an administrator to the database.
Production Instance	Use to go-live with any Service.	Customer has no access to the VMs or to the SQL Azure associated with this environment.

2. Downtime has the meaning given to it in the SLA.

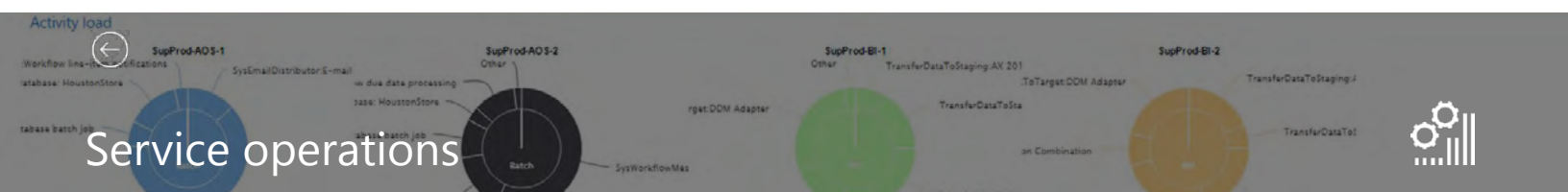


Table 6 details the different levels of access for different Microsoft administrators.

Table 6. Microsoft's administrator access

Administrator	Customer data
Operations responses team (Limited to key personnel only)	Yes, granted by support ticket. Access is audited and limited to the duration of the support activity.
Microsoft Customer Support Services	No direct access. Customer may use screen sharing to work with support staff to debug issues.
Engineering	No direct access. Operations response team may use screen sharing to work with engineering to debug issues.
Others in Microsoft	No access.

Monitoring and incident management

Monitoring

Microsoft has invested in an extensive toolset to monitor and diagnose Customers’ production environments. Microsoft monitors Customers’ production environments 24 hours a day, 7 days a week. Customer must monitor its Production Instances for application configurations and application errors as described in **Table 7**.

Table 7. Monitoring responsibilities

Microsoft's responsibilities	Customer's responsibilities
<ul style="list-style-type: none">• Availability monitoring for the service.• Continuous monitoring and alerts through health metrics and watchdogs for critical components such as AOS, Batch, DIXF, Retail, Management Reporter.• Monitoring for performance degradation caused by infrastructure services (AAD, Azure, SQL etc.).• In the event Microsoft determines that a single process or batch job is causing aberrations, these will be thwarted after communication with the Customer.	<ul style="list-style-type: none">• Monitor changes to application configurations and customizations that can cause functional and performance issues.• Application errors need to be diagnosed using the monitoring tools.• Diagnose user reported performance aberrations using these tools.• Inform Microsoft in the event that there are expected load on the system beyond projected peak usage.• In the event an Service is unavailable in the Production Instance, Customer can create a “Production down” customer support request using LCS.



Incident management

Microsoft responds to and resolves Incidents based on the severity levels set forth in **Table 8.1** and **Table 8.2**. Microsoft's Incident severity levels can be changed during initial assessment of the Incident and as more information about the impact and scope becomes available. If the Incident is mitigated, then the Incident severity remains unchanged.

22

Table 8.1. Severity Level Description

Classification	Description
Severity 0 (Sev-0) Catastrophic	<ul style="list-style-type: none"> Catastrophic event in which all functions of a service in a region are down or inaccessible. <p>Note: Sev-0 Incidents normally start as Sev-1, then get upgraded with management approval based on assessment of impact type/scope.</p>
Severity 1 (Sev-1) Critical	<ul style="list-style-type: none"> Severe outage of a Service caused by confirmed systemic problem, resulting in a broad scope of impact, requiring a Technical Control Bridge and engagement from applicable engineering teams. Suspected breach of a security or privacy boundary.
Severity 2 (Sev-2) Urgent	<ul style="list-style-type: none"> Service outage with narrow scope of impact (> 25% customers). Degradation of customer experience caused by confirmed systemic event with broad scope (> 25% customers). Service outage with limited scope of impact (single organization or subset of users).
Severity 3 (Sev-3) Moderate	<ul style="list-style-type: none"> Degradation of customer experience caused by confirmed systemic event with narrow scope.
Severity 4 (Sev-4) Non-SLA Impacting	<ul style="list-style-type: none"> Monitoring or Customer reported incidents requiring action to avoid potential service impact. General maintenance events with no Customer impact. Standard service change requests.

Table 8.2. Incident Scope and Severity Level Impact

Impact scope	Entire geo OR > 25% of global footprint	1 Customer OR subset of users belonging to one Customer
Incident impact		
Service is unavailable	Sev-1	Sev-2
Service is usable only through a workaround or critical subset feature is malfunctioning	Sev-2	Sev-3
Degradation of performance, or non-critical subset feature is malfunctioning	Sev-3	Sev-4
Incidents requiring action to avoid potential impact or service disruption	Sev-3	Sev-4

See Table 8.1 for definition of Severity 1, Severity 2, Severity 3, and Severity 4



Business continuity with high availability and disaster recovery

Customer's Production Instances include High Availability (HA) and Disaster Recovery (DR) features.

23

- **High Availability.** HA functionality provides ways to prevent Downtime caused by the failure of a single node within an Azure datacenter. Each Service's cloud architecture uses Azure availability sets for the compute tier to prevent single-point-of-failure events. HA for databases is supported through Azure SQL (a platform-as-a-service (PaaS) offering from Microsoft).
- **Disaster Recovery.** DR features protect each Service against outages broadly impacting an entire Azure datacenter and include the following:
 - Azure SQL active-geo replication for primary databases, with a Recovery Point Objective (RPO) estimate of ≤ 5 seconds.
 - Geo-redundant copies of Azure blob storage (containing document attachments) in other Azure regions.
 - Same secondary region for the Azure SQL and Azure blob storage replications.

The primary data stores are supported for replication. This means that components for each Service, such as Management Reporter and Entity Store, use transformed data from the primary database, which need to be generated after the recovery site has been setup and service started. Customer code artifacts and recovered data stores is used to re-deploy the site, with a Recovery Time Objective (RTO) of up to 10 hours. This will enable state replication of the compute nodes along with networking and other components to set up the secondary site using the recovered data stores. In the event DR is utilized to recover Customer's Production Instance, each of Microsoft and Customer will perform the responsibilities described in **Table 8.1** and **Table 8.2**.

**Table 9.** Responsibilities for Disaster Recovery

Microsoft's responsibilities	Customer's responsibilities
Microsoft provisions a secondary environment in the Azure paired datacenters at the time of deployment of the primary Production Instance. See the business continuity and disaster recovery (BCDR): Azure Paired Regions here https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions for details.	None.
Microsoft enables Geo Redundancy of SQL and Azure Storage at the time of deployment of the primary Production Instance.	None.
Microsoft backs up the VMs regularly using Azure backup.	None.
On outage, Microsoft determines if a failover needs to be executed for Customer and if there will be a data loss. Data loss can be up to 5 sec. For details, see Azure SQL Database Geo-Restore here: https://azure.microsoft.com/en-us/blog/azure-sql-database-geo-restore/	Customer may need to provide written sign-off to trigger the failover in the event of data loss.
In the event of a data loss, Microsoft will send a request to Customer asking for its sign-off on a failover.	
The applicable Service will be operated in limited mode on failover. Update maintenance cannot be triggered in failover mode.	Customer cannot request package deployments or other regular maintenance requests in failover mode.
Microsoft fails back to the Production Instance in the primary Azure region when the datacenter becomes operational. Normal operations are resumed.	Customer may need to sign-off on fail back to the Production Instance in the primary Azure region.

Application support offerings

Microsoft offers VL customers three support plans: Premier, Professional Direct, and the support included in the subscription. The level of support differs per plan and highlights are provided in the **Table 10**.

Table 10. Key VL support service features

Service feature	Premier	Professional direct	Subscription
Unlimited break/fix incidents	●	●	●
24x7 support	●	●	Local business hours
Fastest response times	<1 hour	<1 hour	Next business day

Process to engage support

In case of incidents with Finance and Operations, Customers can submit support incidents to Microsoft by phone or through LCS. CSS will handle incidents depending on the Customer's support plan and severity of the incident as designated by CSS.

Service Level Agreement

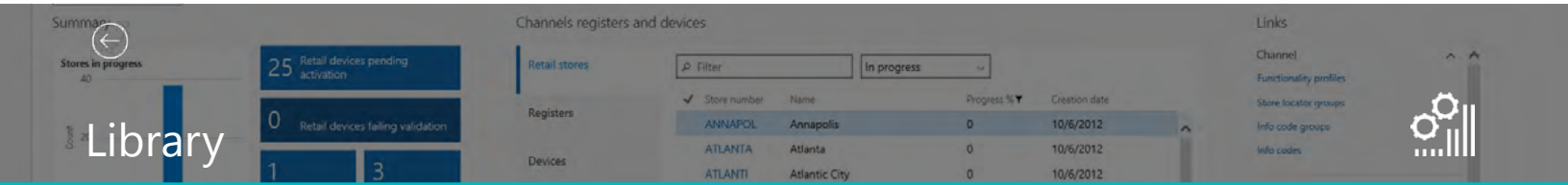
Microsoft is committed to an availability of 99.9% per month of the service. If Microsoft does not achieve and maintain the Service levels for Finance and Operations described in the SLA, then Customer may be eligible for a credit towards a portion of its monthly service fees for Finance and Operations. See the "Claims" section of the SLA for details on how to initiate a service credit.

Service Level Agreement

SLA



Library



More information about Finance and Operations can be found in the sources published below.

Trust Center
Information on where your Finance and Operations data is stored, plus additional information on privacy, compliance, and security procedures

[Learn more](#)

Online Service Terms
Terms and conditions of Microsoft's services

[Learn more](#)

Service Level Agreement
Service Level Agreement

[Learn more](#)

Update policies
Online updates

[Learn more](#)

Online Services lifecycle support policy
Support policy

[Learn more](#)

Licensing guide
Overview of service licensing

[Learn more](#)

Customer support
Details about the three support plans for customers

[Learn more](#)

Dynamics Lifecycle Services
Access LCS

[Learn more](#)



Definitions

Definitions

The following table contains the meaning of terms used in this document.

Click the links below for more information.

Azure region

A geographical region where one or more Azure datacenters exist; for example, US and Europe.

Business Process Manager (BPM)

A tool in LCS to help complete a fit-gap analysis for a given implementation using business process definitions as defined in APQC and their support within Finance and Operations.

Cloud Solution Provider (CSP)

Partners who are part of Microsoft's CSP program and provide Customers with value-added cloud services, Customer support, one invoice, and Customer management at scale.

Customer

A business entity that consumes Finance and Operations and is represented by a tenant in Office 365 service.

Development environment

Tenant used for developing customizations.

Downtime

Any period of time when end users are unable to login to their Active Tenant, due to a failure in the unexpired Platform or the Service Infrastructure as Microsoft determines from automated health monitoring and system logs. Downtime does not include Scheduled Downtime, the unavailability of Service add-on features, the inability to access the Service due to your modifications of the Service, or periods where the Scale Unit capacity is exceeded.

Implementation Partner

The partner that Customer choses to customize, configure, implement, and manage its Finance and Operations solution.

Microsoft Dynamics Lifecycle Services (LCS)

Online portal for lifecycle management of Finance and Operations from trial to implementation to post-production management and support.

Microsoft Online Services Terms (OST)

The OST contains terms that apply to Customer's use of Online Services.

Microsoft Service Engineering (DSE)

Dynamics Service Engineers team responsible for managing public cloud operations.

Cloud Solution Provider

Lifecycle Services

Online Services Terms



Definitions

Microsoft Customer support (CSS)

Microsoft's support team dedicated to providing quality service for Finance and Operations.

Non-production instance

Any of the following instances of a Service that are used by Customer for validating customizations and other development tasks:

- **Sandbox Tier 1:** Developer Instance
- **Sandbox Tier 2:** Standard Acceptance Testing Instance
- **Sandbox Tier 3** Add-on through Sandbox Tier 5 Add-on

Production environment

Instance of Finance and Operations used by Customer for managing its "live" daily transactions.

Sandbox/staging environment

Instance of Finance and Operations used by Customer for validating customizations and other development tasks.

Service

The core services which are included in Microsoft Dynamics 365 for Finance and Operations; Microsoft Dynamics 365 for Retail; or both.

Service Level Agreement for Microsoft Online Services (SLA)

The SLA applies to Microsoft's Online Services, including Finance and Operations.

Service Level Agreement

Support incident

An issue with the Finance and Operations that Customer encounters while using the service.

Update request

Request raised to Microsoft for specific update.

User

A single person consuming Finance and Operations, which is associated with a Customer's tenant.

Virtual machine (VM)

A persistent instant type that can be deployed individually or as part of 2 or more virtual machines deployed across a different collection of servers that share common resources, such as power and network connectivity, to avoid a single point of failure.

Volume licensing (VL)

Microsoft's licensing program for organizations to acquire Microsoft's software or cloud services.

Volume licensing

© 2018 Microsoft Corporation. All rights reserved.

This document is provided "as-is." The information and views expressed in this document, including URL and other Internet Web site references, are current as of the publication or revision date and may change without notice. You bear the risk of using it.

This document is provided for informational purposes only and cannot be incorporated within, or attached to, any type of an agreement. This document is not intended to be a service contract, and does not commit Microsoft, its channel partners, or the customer to any features, capabilities or responsibilities mentioned herein. As used in this document, references to "partner" refer solely to marketing relationships and do not refer to or imply a partnership or any other legal relationship.

The furnishing of this document does not provide you with any legal rights to any intellectual property in any Microsoft product or service. You may copy and use this document for your internal, reference purposes only.



Microsoft Dynamics 365 for Finance and Operations