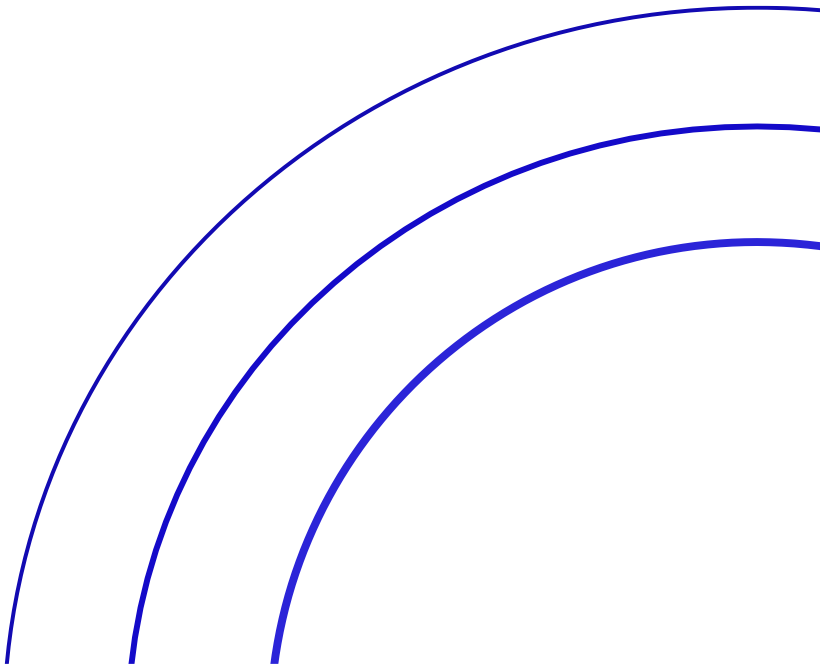
Managed M365 Service Description



Document Control

TITLE:	**Managed M365 Service Description**	**DOCUMENT REF NO:**	QMS REC105
DESCRIPTION:	This document defines the services provided by Calligo's Managed M365service		
OWNER/ AUTHORITY:	Director, Operations Management	**VERSION NO:**	1.1
DOCUMENT CROSS REFERENCE:	N/A	**VERSION DATE:**	25/11/2022
DISTRIBUTION METHOD	Email and Website	**DOCUMENT CLASSIFICATION**	Internal

DOCUMENT OWNER & APPROVAL
The Director, Operations Management, is the owner of this document and is responsible for ensuring that this service description is reviewed in line with the review requirements of Calligo's Information Security Management System, Project Management Frameworks as well as the guidance and requirements of the CSSF.
Approved by the VP, Cloud Operations Officer, Calligo ("Entity") on 25 November 2022

CHANGE HISTORY RECORD				
VERSION	**DESCRIPTION OF CHANGE**	**AUTHOR**	**APPROVAL**	**DATE OF ISSUE**
1.0	Original Version	Director, Operations Management	VP, Cloud Operations	25/11/22
1.1	Remove Service Locations table and add link to external Service Locations document.	Director, Operations Management	VP, Cloud Operations	10/01/23

1. Service Overview

This document defines the services provided by Calligo's Managed M365service. The Managed M365service is one of a suite of services within the Calligo Operating Model.

Managed Desktop is a managed Endpoint service that covers OS patching (Feature Updates, Quality Updates, Servicing Stack Updates, Critical and Security Updates) to maintain OS currency and Security for in support Windows OS versions.

2. Service Inclusions

1.1. CO-ITSM-SD

This service leverages an ITSM platform and trained Level 1 Service Desk Analysts to cover activities that provide a client facing Service Desk

1.2. CO-ITSM-M365APP

This service provides M365 application support and patching activities via tooling or M365 Portal and Servicing Channels

3. Service Provisions

1.3. CO-ITSM-SD

1.3.1. Inclusions

CO-ITSM-SD	
Scope Item	**Description**
Access to the Calligo ITSM platform	24/7 access to the Calligo ITSM platform that provides capabilities for clients to raise new support tickets and to access open or historic support tickets.
Telephone Support	Access to the Calligo Service Desk via the issued telephone contact numbers during regional Business Hours only.
First Line Fix	Access to the Calligo L1 Service Desk Analysts for first line fix or resolution.

1.3.2. Exclusions

CO-ITSM-SD	
Exclusion Item	**Description**
24/7 Telephone Support	This is a chargeable addition.
Onsite support	All support delivered via the Service Desk offering is remote.

1.4. CO-ITSM-M365APP

1.4.1. Inclusions

CO-ITSM-M365APP	
Scope Item	**Description**
Remote Administration	Microsoft 365 application download and basic application support limited to the User being able to open and use the application on supported workstations or mobile devices (as defined in the Supported Applications List
Microsoft 365 Health Monitoring	Monitoring and client alerting for M365 systemic outages and impact

Microsoft 365 License Provisioning	Assignment of relevant end user licenses.
Microsoft 365 User Management	The following activities are supported: • Moves • Adds • Changes Deletes
Supported Applications	The following M365 applications are included for support: • Microsoft Word • Microsoft Excel • Microsoft PowerPoint • Microsoft Teams • Microsoft Outlook • Microsoft OneDrive • Microsoft SharePoint
Microsoft 365 mailbox management	Configuration of forwarding rules, permissions, and aliases

1.4.2. Exclusions

CO-ITSM-M365APP	
Exclusion Item	**Description**
Required Licensing	This element of service requires SI: **CO-SW-LICENSE**
Provision and management of Two-Factor Authentication (2FA)	This element of service requires SI: **CO-CP-MFA**
Unsupported Applications	The following M365 applications are not included for support: • Microsoft Access • Microsoft Publisher • Microsoft Intune • Microsoft Azure Information Protection • Microsoft Exchange (Exchange Online) • Microsoft Teams Voice (Requires SI: **CO-ITSM-BV**) • PowerBI

4. Roles and Responsibilities

The table below provides a responsibility matrix for the core Managed M365elements:

Service Activities – Core Elements	Calligo	Customer
CO-ITSM-M365APP		
Microsoft 365 application download and basic application support limited to the User being able to open and use the application on supported workstations or mobile devices (as defined in the Supported Hardware & Software List on Calligo's website)	R, A, C	I
Configuration of the MS Outlook client on supported workstations and mobile devices (as defined in the Supported Hardware & Software List on Calligo's website).	R, A, C	I
Microsoft 365 health monitoring	R, A, C	I
Microsoft 365 license provisioning	R, A	C, I
Microsoft 365 user management (moves, adds, changes, deletes)	R, A	C, I
Microsoft 365 mailbox management (forwarding, permissions, aliases)	R	A, C, I
Business application verification, maintenance, and testing	C, I	R, A
(M365 Application Patching Tooling) Patch Deployment	R, A, C	
Defining standard recurring deployment schedules, exclusions, and targets	C, I	R, A
(M365 Application Patching Tooling) Compliance measurement for SLO/SLA purposes	R, A, C	I
Add and remove systems to scope	R, A	C, I

Review released list of patches from Microsoft and provide customer notification prior to scheduled installation	R, A	C, I
(M365 Application Patching Tooling) Identify patches to be excluded and approve list of patches for deployment	C, I	R, A
Identify business areas that require patch reporting and provide contact information for recipients	C, I	R, A
(M365 Application Patching Tooling) Run reports on a scheduled basis and provide malware detection alerts	R, A	C, I
(M365 Application Patching Tooling) Identify patches to be excluded and approve list of patches for deployment	C, I	R, A
(M365 Application Patching Tooling) Identify business areas that require patch reporting and provide contact information for recipients	C, I	R, A
CO-ITSM-SD		
Raising support requests	R	R, A
Contacting Calligo Service Desk via telephone for P1 Support Requests	I	R, A
Correctly assigned the right category and priority to all incoming support requests	R, A	C, I
Providing full and detailed information when creating new support requests	I	R, A
Providing detailed and regular ticket updates	R, A	I
Responding to all ticket updates where additional information or testing is requested from Calligo Service Desk	I	R, A
Providing prompt confirmation of ticket closure agreements.	I	R, A

R=Responsible, A=Accountable, C=Consulted, I=Informed

5. Reporting

The table below provides details on the additional Monthly Reporting and Analytics for Managed M365 that are included in the core service:

Service Item	Reporting Item	Description	Frequency
CO-ITSM-M365APP	M365 usage	Mailbox sizing, OneDrive sizing and assigned licenses.	1 Monthly
CO-ITSM-M365APP	OneDrive External Sharing	Lists of current external OneDrive shares	1 Monthly
CO-ITSM-M365APP	Security and Compliance reporting	Office 365 Secure Score, DLP Policy	1 Monthly
CO-ITSM-M365APP	(M365 Application Patching Tooling) Asset lists (Deployment Collections)	List of all assets currently in scope as well as their current collection memberships and deployment windows	1 Monthly. Sent a day after Patch Tuesday
CO-ITSM-M365APP	(M365 Application Patching Tooling) Patch Advisory	The report lists all required patches that are scheduled for deployment.	1 Monthly. Sent a day after Patch Tuesday
CO-ITSM-M365APP	(M365 Application Patching Tooling) Pre-Patch Compliance Report	The report includes compliance summary and a list of non-compliant systems.	1 per deployment. Sent prior to deployment.
CO-ITSM-M365APP	(M365 Application Patching Tooling) Asset Compliance State (Current Cycle)	Current patch compliance state for the current month deployments.	1 Monthly after deployment completion
OS-ITSM-M365APP	(M365 Application Patching Tooling) Asset Compliance State (Cumulative Cycle)	Current patch compliance state for the cumulative (OS in support Date through Current – 1) deployments.	1 Monthly after deployment completion

6. Data Residency

Calligo Data Residency

7. Service Requirements

Service Item	Requirements Item
CO-ITSM-M365APP	All applicable M365 licenses
CO-ITSM-M365APP	Current in support or Extended support Windows OS assets.
CO-ITSM-M365APP	Deployment of Datto RMM agent and relevant firewall / access configurations for each in scope asset
CO-ITSM-M365APP	An agreed and defined re-occurring maintenance window for automated patch installation and remediation activities
CO-ITSM-M365APP	Reboots are permitted within the agreed maintenance windows.
CO-ITSM-M365APP	Outbound internet access for reporting and patching.
CO-ITSM-SD	Client is provided information on support access methods
CO-ITSM-SD	All Priority 1 incidents are logged, and the client must follow up with a telephone call into support.

8. Access Requirements

Requirements Item
Access to hosted servers is either by virtual private network (VPN) or dedicated communication links depending on Client requirements.
Administrative access to all assets in scope as required for remediation actions
Service account for Datto RMM agent activities

9. Support Locations

Calligo Support Locations

10. Service Catalogue Request Items

Catalogue Item	Fulfilment Time	Qualifying Criteria	Included Requests
Mailbox Migrations	40BHR	Customer supplied list of mailboxes to migrate. May require project scheduling depending on size and scope of request.	1 Monthly
Add/Remove asset from scope	8BHR	Supplied list of assets	1 per week

11. Standard SLO's

Service-Level-Agreement.pdf (calligo.io)

12. Related Documents

Supporting documents for this service:

Any clients onboarding to Calligo will require the following document as an introduction to service

13. Optional Services

In addition to the Managed M365service, Calligo can provide the following service items as optional add on services for Managed M365:

Cloud Protect MFA

1. Cloud Protect MFA – CO-CP-MFA
    a. This service Leverages native or third-party MFA solutions
    b. Service Elements Scope

<table>
<tr><th>Service Item</th><th>Service Item Reference</th><th>Description</th></tr>
<tr><td>Cloud Protect MFA</td><td>CO-CP-MFA</td><td>This service Leverages native or third-party MFA solutions
Service Elements Scope:<table><tr><th>SCOPE ITEM</th><th>DESCRIPTION</th></tr><tr><td>Enrolment</td><td>New device or user enrolment</td></tr><tr><td>Application integration</td><td>Integrate Calligo-supplied MFA with natively supported applications</td></tr><tr><td>Remediation of MFA services issues</td><td>Remediation of systemic system issues</td></tr></table>Service Provision Excludes<table><tr><th>EXCLUSION ITEM</th><th>DESCRIPTION</th></tr><tr><td>Client network connectivity</td><td>An active internet connection is required on the mobile device to receive MFA push notifications</td></tr><tr><td>Custom application integration</td><td>Custom applications developed by the customer or contracted organization</td></tr><tr><td>End user device</td><td>Device issues unrelated to MFA</td></tr><tr><td>Credentials</td><td>First-factor authentication (e.g., password) issues</td></tr></table>Service Catalog Request Items</td></tr>
<tr><td>Cloud Protect Email Hygiene</td><td>CO-CP-EH</td><td>This service adds email hygiene and mail content filtering to Exchange online.</td></tr>
<tr><td>M365 Threat Protection</td><td>CO-ITMS-M365TP</td><td>This service adds AV and Malware protection on each endpoint in scope as well as monitoring and initial remediation activities.</td></tr>
<tr><td>CloudProtect Web Filtering (Sophos)</td><td>CO-CP-WFS</td><td>This service adds web filtering as required,</td></tr>
<tr><td>M365 Business Voice</td><td>CO-ITSM-BV</td><td>This service provides support for Teams Business Voice for Cloud PBX or related PSTN services.</td></tr>
</table>

Licensing	CO-SW-LICENCE	Calligo's Licencing Service provides Application, OS and Appliance licensing procurement as well as Provisioning and Management of service subscriptions. Reporting of license usage as well as monthly Invoicing provides detailed status of all current client licensing.
365 User Protected User	CO-BAAS-365USER	Calligo's M365 Application and data level backups provides data assurance for all supported M365 applications.
Service Delivery Manager	CO-ITSM-SDM	The Service Delivery Manager will be responsible for the business as usual and account management relationship. This will include service reviews, point of escalation, responsible for Information Technology Infrastructure Library (ITIL) practice adherence, interfacing with third-party suppliers also participating under the customer's Service Integration and Management model and ensuring that Calligo meets or exceeds Service Level Objective (SLO) targets.
Technical Account Manager	CO-ITSM-TAM	The Technical Account Manager will be responsible for the technical collaboration between the customer and Calligo support teams and will play a key role in technical service improvement, managing deployment of new services or configuration changes, ensuring optimal performance and uptime of the application stack, and interfacing with third-party suppliers as required under the customer's support model.

14. Auxiliary Services

1.5. Service Onboarding & Transition

To launch Managed M365 service successfully, service design, onboarding and transition will be required to prepare and test both the environment and the managed services processes. Calligo will undertake several workshops to discuss and confirm each element of the service to ensure all parties are aware of roles and responsibilities in advance of service launch.

Service transition and onboarding covers areas such as ticket management setup, platform readiness with knowledge share, and finalising all ITIL practices. A test and acceptance criteria are captured and signed off, to allow for the Managed M365 service to commence.

After service launch, Calligo uses a formal service transition framework as the basis to carry out acceptance into service procedures, for new services landing into managed services. We typically engage at the initial stages of a project to ensure service operation adoption and readiness is planned and carried out correctly. This materializes as follows:

- To review designs, build and test artefacts to ensure supportability.
- Attend change review boards to gain early sight of changes by way of knowledge acquisition.
- To witness and validate designs and builds are delivered as proposed and intended.
- Complete operational into service documentation, training and runbook enablement, which is required as part of the service hand-over.

1.6. Change Request and Change Control Process:

All infrastructure changes introducing risk to the environment will require change control which includes, but not limited to, Microsoft Security Patching, Infrastructure Upgrades, Deployments, Configuration Item status change. This can be generated from maintenance or an event such as an

upgrade required on the system released by Third Party vendors, requested by the customer, or from a monthly release of security patches.

Where possible Standard Changes will be used with minimal risk, repeatable implementation steps, and prior approval from the customer in the form of an email.

An Emergency, or unplanned, change process will be raised to resolve a Priority 1 or 2 incident or to implement an emergency Security Patch. This accelerates the time to implement and resolve.

All Requests for Change will be reviewed internally, assessed internally and authorized or rejected through Calligo ITSM tool.

1.7. Superseded patch scenarios

This relates to the behavior which occurs when a newer update is released after the patch cycle has started:

- **Revisions -** When a metadata only revision to an update is made, the update identified in the deployment is still installed. There is no new update released by the vendor for this. Updates with material changes (binaries) are considered superseded updates and the supersede rule applies.

- **Supersede -** When the update source marks an included patch as superseded, the superseded update will not be installed. The newer update will need to be included at a future patch cycle.

- **Expiration -** At the time of installation, when a patch has been included for installation but is marked as expired by Windows Update, the install of that patch will not occur. The asset will report compliant since the patch no longer meets the requirements to install. Where a newer update becomes available it will need to be included on a future patch cycle.