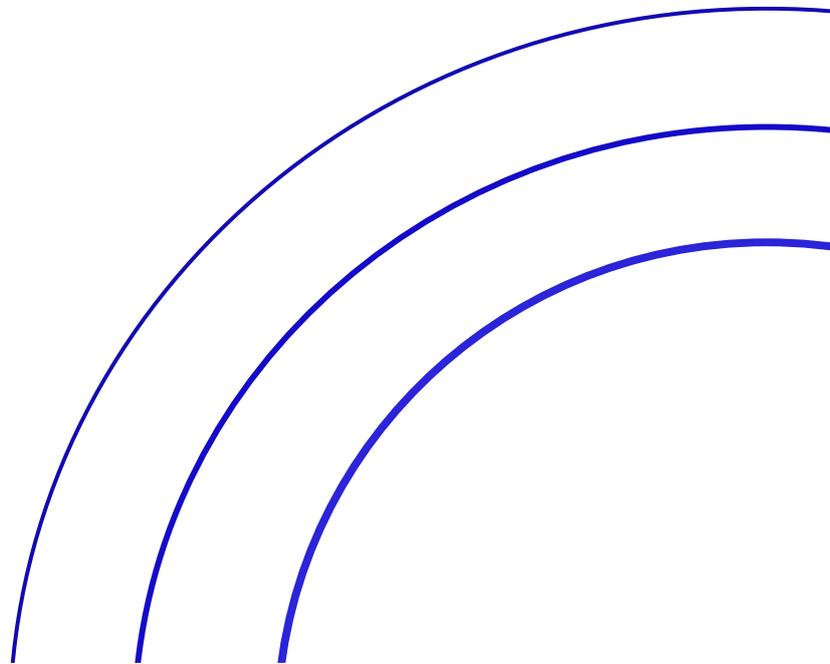




**Managed M365 Service
Description**



Document Control

TITLE:	Managed M365 Service Description	DOCUMENT REF NO:	QMS REC105
DESCRIPTION:	This document defines the services provided by Calligo's Managed M365 service		
OWNER/ AUTHORITY:	Director, Operations Management	VERSION NO:	1.6
DOCUMENT CROSS REFERENCE:	N/A	VERSION DATE:	15/09/2023
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
1.2	Extension of Optional Service items	Director, Operations Management	VP, Cloud Operations	31/01/23

1.3	Updated supporting documentation links	Director, Operations Management	VP, Cloud Operations	20/02/23
1.4	Updated Optional Service Items	Director, Operations Management	VP, Cloud Operations	11/09/23
1.5	Removed one of the Optional Service Items	Director, Operations Management	VP, Cloud Operations	12/09/23
1.6	Updated scoped items for optional service items – BaaS – Office 365	Director, Operations Management	VP, Cloud Operations	15/09/23

1. Service Overview

This document defines the services provided by Calligo's Managed M365 service. The Managed M365 service is one of a suite of services within the Calligo Operating Model.

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: <ul style="list-style-type: none"> • Moves • Adds • Changes

	Deletes
Supported Applications	The following M365 applications are included for support: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 M365 elements:

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.

[Calligo – Welcome to Support for Clients](#)

13. Optional Services

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

13.1 Cloud Protect MFA

This service leverages native or third-party MFA solutions

Service Elements Scope

SCOPE ITEM	DESCRIPTION
Enrolment	New device or user enrolment
Application integration	Integrate Calligo-supplied MFA with natively supported applications
Remediation of MFA services issues	Remediation of systemic system issues

Service Provision Excludes

EXCLUSION ITEM	DESCRIPTION
Client network connectivity	An active internet connection is required on the mobile device to receive MFA push notifications
Custom application integration	Custom applications developed by the customer or contracted organization
End user device	Device issues unrelated to MFA
Credentials	First-factor authentication (e.g., password) issues

Service Requirements

REQUIREMENTS ITEM
Mobile device running current iOS or Android operating system, with internet connectivity (necessary to receive push notifications)
Client server to run MFA authentication proxy (where applicable)

Access Requirements

REQUIREMENTS ITEM
Administrative access to the MFA management interface. This is necessary to configure integrations, enrol users, and troubleshoot issues
Administrative access to server running authentication proxy. This is necessary to troubleshoot connectivity and authentication failures
Administrative access to directory server and any systems utilizing the authentication proxy. This is necessary to troubleshoot authentication failures.

Data Residency

RESIDENCY ITEM	DESCRIPTION	SYSTEM	STORAGE LOCATION
MFA user database, mobile device information, authentication history	All information necessary to provide the MFA service including usernames and permissions, basic device info (e.g., model and OS), phone number, authentication logs	System 1 – Calligo MFA solution	EU
		System 2 – Microsoft 365	https://azure.microsoft.com/en-gb/global-infrastructure/geographies/#overview

Service Catalogue Request Items

CATALOG ITEM	FULFILMENT TIME	QUALIFYING CRITERIA	INCLUDED REQUESTS
New user enrolment	8BHR	Enrol a new user in MFA	5 per week
New device enrolment	8BHR	Enrol an existing user's new device	5 per week
Unlock user account	4BHR	Unlock a locked account	5 per week
Lock user account	8BHR	Prevent a user signing in	5 per week
Integrate application	24BHR	Integrate MFA with a supported application	1 per month
Reporting	24BHR	Generate MFA activity report	1 per week

Standard Reporting

REPORTING ITEM	DESCRIPTION	FREQUENCY
Authentication Log	Report detailing user activity, both successful and unsuccessful authentication attempts, locked out accounts	1 per month if requested
Deployment Progress	Enrolled, active, unenrolled, inactive users	1 per month if requested

RACI Table

SERVICE ACTIVITIES	Calligo	Customer
Enrolment of new users and new devices	R, A	R, A
Unlocking accounts	R, A	C
Account lockout	R, A	R
Application Integration	R, A, C	C, I
Remediation of systemic issue	R, A	C, I

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

13.2 Cloud Protect Email Hygiene

SCOPE ITEM	DESCRIPTION
Inbound Sender Policies	Rule definition for sender domain, IP, and geolocation whitelisting and blacklisting, SPF/DKIM/DMARC sender verification, AV and reputation-based e-mail scanning
Message categorization actions	Assign filtering actions by detected message type, including Corporate, Transactional, Marketing, Mailing list, social media, and Bulk E-mail
Custom block/quarantine thresholds	Scanned mail is assigned a spam confidence score. Thresholds can be assigned to block or quarantine dependent on message score.
Phishing policies	Detection of phishing or fraudulent mail, typo squatting protection, URL scanning
Message content policies	Rule definition for permitted and denied attachment formats, encrypted documents, message headers and body content, DLP (outbound only)

Rate control policy	Limit x messages sent or received by an IP address within a 30-minute period.
E-mail Quarantine	Release of blocked messages to recipients' mailboxes, quarantine notifications and self-service quarantine management

Service Provision Excludes

EXCLUSION ITEM	DESCRIPTION
Per-user filtering	Mail policies are assigned globally to the mail domain
DNS	Management of DNS records required for mail delivery (MX, TXT, SRV, etc.)
Client Mail Server	Administration or troubleshooting client mail server
Recipient Mail Server	Administration or troubleshooting for mail routing or delivery issues external to the spam filter
Intra-site messaging	Message filtering cannot apply to internal mail

Service Requirements

REQUIREMENTS ITEM
Mail Exchange (MX) records in DNS must point only to the spam filtering service.
A mail server is necessary for delivery of received mail
The firewall must accept SMTP connections to/from the spam filtering service (TCP ports 25, 587, 465)
Outbound message scanning requires entry of a smart host server address on the client mail server

Access Requirements

REQUIREMENTS ITEM
No system access is required outside the cloud-hosted spam filtering platform

Data Residency

RESIDENCY ITEM	DESCRIPTION	SYSTEM	STORAGE LOCATION
Appliance	Security Appliance	Endpoint Security platform	Multiple Options Available

Service Catalogue Items

CATALOG ITEM	FULFILMENT TIME	QUALIFYING CRITERIA	INCLUDED REQUESTS
Sender Whitelist/Blacklist	24BHR	Sender's e-mail address or domain, action (allow or block)	5/week
Block region or language	24BHR	Countries and character sets to block	1/week
Custom Realtime blackhole list	24BHR	Server address or IP	1/week
Authentication exemption	24BHR	Sender's domain or IP address, exemption (SPF, DKIM, DMARC, PTR)	5/week
Release message (within 30 days)	24BHR	Sender, recipient, approximate date and time message was blocked	5/week

Filtering threshold change	24BHR	Desired spam confidence score to trigger message block or quarantine	1/week
Content policy change	24BHR	Content patterns to allow or deny, e-mail message samples	1/week
Phishing policy change	24BHR	Phishing detection action (Ignore, Quarantine, Block)	1/week
URL scan exemption	24BHR	Domain to exempt from URL protection	1/week
Outbound DLP Policy	24BHR	Data format or category (e.g. HIPAA), allow or deny	1/week
Rate limit change	24BHR	Desired rate limit or sender exemption	1/week
Quarantine notification enablement or schedule change	24BHR	Desired quarantine notification frequency and schedule	1/month
Assign Client Role	24BHR	User, required role (helpdesk or admin)	1/month

Standard Reporting

REPORTING ITEM	DESCRIPTION	FREQUENCY
Inbound Traffic	Summary of inbound messages and scan results (Allowed, Blocked: Rate Control, Spam, Virus, etc.)	1/month if requested
Outbound Traffic	Summary of outbound messages and scan results (Allowed, Blocked: Rate Control, Spam, Virus, etc.)	1/month if requested
Top Senders	Highest frequency senders and their delivery results (Allowed or Blocked: Rate Control, Spam, Virus, etc.)	1/month if requested
Top Recipients	Highest frequency recipients and their delivery results (Allowed or Blocked: Rate Control, Spam, Virus, etc.)	1/month if requested

RACI Table

SERVICE ACTIVITIES	Calligo	Customer
Mail filter policy changes	R, A	A, C
User Quarantine		R, A
Blocked Message release	R, A	A, C
Client Admin assignment	R, A	A, C, I

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

13.2 M365 Threat Protection

This service leverages Sophos

Service Elements Scope

SCOPE ITEM	DESCRIPTION
Configuration	Deployment of Antivirus and Monitoring applications to all End Points Configuration of automatic update timing Configuration of End Point Protection e.g., Exemptions, End Point specific requirements, Computer/Endpoint Groups Initial Compliance Audit and Antivirus/Antimalware scans on all End Points Application Control Policies Web Control Policies Data Loss Prevention Policies
Initial Remediation	Remediation of any infection indicated endpoints
Define Reports	Setup initial reporting and provide access to client
Scanning	End user device scanning & remediation
Configuration	Deployment of Antivirus and Monitoring applications to all End Points Configuration of automatic update timing Configuration of End Point Protection e.g., Exemptions, End Point specific requirements, Computer/Endpoint Groups Initial Compliance Audit and Antivirus/Antimalware scans on all End Points Application Control Policies Web Control Policies Data Loss Prevention Policies

Service Provision Excludes

EXCLUSION ITEM	DESCRIPTION
End-of-Life OS	Microsoft and Apple OS that have passed end of support date, and no extended support agreement exists
Mobile devices	Web filtering does not extend to mobile phones (e.g., iOS or Android OS)
Personal devices	Personally owned devices are excluded from web filtering
Unsupported OS	Other OSes such as Linux, non-Windows hypervisors, or embedded systems
Personal Devices	Personally owned devices are excluded from End Point threat protection

Service Requirements

REQUIREMENTS ITEM
Endpoint security software must be installed to all protected assets
The Endpoint agent must be able to frequently connect to the internet in order to receive timely updates/policies and protection.

Access Requirements

REQUIREMENTS ITEM
Administrative access to in-scope devices to install Endpoint Security software

Data Residency

RESIDENCY ITEM	DESCRIPTION	SYSTEM	STORAGE LOCATION
Web control policy and user access history	Defined web control policies, user access and history	Endpoint Security platform	EU

Service Catalogue Items

CATALOG ITEM	FULFILMENT TIME	QUALIFYING CRITERIA	INCLUDED REQUESTS
Single Asset level Scan	2BHR	Asset/endpoint name	5/month per 50 users
Full Environment Asset Scan	8BHR	Group or environment name	4/month (as requested)
Computer Group Creation	24BHR	Desired computer group name	1/week
Computer Group Update	24BHR	List of computers required in the group.	1/week
Computer Group Policy Creation	24BHR	Description of required policy	1/month
Computer Group Policy Update	24BHR	Description of required policy changes	1/week
Create/Update Scanning Exclusion Policies	24BHR	Description of required location/file exclusions	1/week

Standard Reporting

REPORTING ITEM	DESCRIPTION	FREQUENCY
Endpoint Protection Summary	Total Threats blocked, Assets protected, Users Protected (Max 30 days)	1/Month
Licenses and Usage	List of Endpoint licenses	1/Month
Computer Report	Online Status, Last User, Last Update, Computer Group, Agent Install Status	1/Month
Websites blocked and warned	Effectiveness of web control policies	1/month

RACI Table

SERVICE ACTIVITIES	Calligo	Customer
Install endpoint security software	R, A, C	A
Single Asset Level Scan	R, A	C, I
Full Environment Asset Level Scan	R, A	C, I
Request Computer Groups/Change	C	R, A
Computer Group Creation/changes	R, A	I
Request Policy Creation/Updates	C	R, A
Policy Creation/Updates	R, A	I
Report Creation	R, A	I
Initial Virus/Malware Remediation	R, A	C, I

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

13.3 M365 Business Voice

This service leverages Microsoft teams Business Voice

Service Elements Scope

SCOPE ITEM	DESCRIPTION
Client-owned phone number porting	Initiate number porting via Admin Teams Centre
Direct dial number assignments / removals	Assign numbers to users and auto attendants
Setup of toll-free or service numbers	Setup auto attendants and assign numbers and licenses to Resource account
Setup and maintenance	<ul style="list-style-type: none"> • Call queues/auto-attendants • Teams Virtual Assistant • Calling policies • International and domestic licensing
Review on-premises conference phone hardware compatibility and make recommendations	Review existing hardware, to check compatibility of hardware, and produce findings report/review with customer
IVR Functionality	<ul style="list-style-type: none"> • Configuration and editing of auto-attendant. • Configure recording messages for auto-attendants. • Configure holidays, Business hours and After hours call routing

Service Provision Excludes

EXCLUSION ITEM	DESCRIPTION
Escalation to Microsoft for anything relating to a CSP subscription not provided by Calligo.	Client is responsible for any direct Microsoft escalations regarding Teams Business Voices services.
Troubleshooting of applications and services not identified as in-scope for this service.	Calligo does not provide support for user's individual Team's preferences and settings
Call Record Messages and templates	Calligo does not provide call recording services for voicemails or auto attendants. This element of service requires SI: CO-ITSM-M365APP
Onsite Service	Onsite visit may be required, at the recommendation of Calligo, if remote assistance is not possible. This element of service requires SI: CO-ITSM-ONSITE

Service Requirements

REQUIREMENTS ITEM
Full 'Microsoft 365 Voice' service item functionality requires one of the following license sets: <ul style="list-style-type: none"> • Option 1 If your business has Microsoft 365 Business Basic/Standard/Premium Licensing, you will require the add-on 'Microsoft 365 Business Voice without Calling Plan' for each user who requires voice calling.

- Option 2
If your business has Microsoft/Office 365 E1/E3 Licensing, you will require the add-on 'Microsoft 365 Phone System' for each user who requires voice calling.
- Option 3
If your business has Microsoft/Office 365 E5 you already have access to the Microsoft Phone System.

Toll Free Numbers:

To use toll free numbers, "Communication Credits" are required to purchase. Toll-free calls are billed per minute and require a positive Communication Credits balance. Initial purchase of Communication Credits requires a minimum spend and can be topped up automatically via credit card or other purchasing agreement. Communication Credits cannot be purchased via CSP, and must be purchased through the Office 365 portal directly

Access Requirements

REQUIREMENTS ITEM

Administrative (Local) access to all assets in scope as required for remediation actions

Data Residency

RESIDENCY ITEM	DESCRIPTION	SYSTEM	STORAGE LOCATION
Call recordings	Call recordings are stored in the OneDrive for Business account of the user who initiates the recording. Teams call recordings are also stored in Azure Media Services.	Microsoft Teams Voice	https://azure.microsoft.com/en-gb/global-infrastructure/geographies/#overview
Voicemails and transcriptions	Voicemails and call transcriptions are both stored in the receiver's Exchange mailbox	Microsoft Teams Voice	https://azure.microsoft.com/en-gb/global-infrastructure/geographies/#overview

Service Catalogue Request Items

CATALOG ITEM	FULFILMENT TIME	QUALIFYING CRITERIA	INCLUDED REQUESTS
New User Request	48BHR	Name, Department	One Weekly
New Auto Attendant Request	48BHR	Name, Purpose, Users	One Monthly

Standard Reporting

REPORTING ITEM	DESCRIPTION	FREQUENCY
Call Usage Reports	Report showing call usage details for users, and auto attendant accounts	One monthly

RACI Table

SERVICE ACTIVITIES	Calligo	Customer
Direct dial number assignments / removals	R, A	C, I
Setup of toll-free or service numbers	R, A	C, I
Setup and maintenance of: <ul style="list-style-type: none"> • Call queues/auto-attendants • Teams Virtual Assistant • Direct routing • Calling policies 	R, A	C, I

<ul style="list-style-type: none"> International and domestic licensing 		
Review on-premises conference phone hardware compatibility and make recommendations	R, A	C, I
IVR Functionality <ul style="list-style-type: none"> Setup and editing of auto-attendant Recording messages for auto-attendant Holidays, Business hours and After hours call routing 	R, A	C, I
Physical phone endpoints (e.g., Phones, headsets, conference systems, etc)	I	R, A, C
Voice call quality troubleshooting	C, I	R, A

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

13.4 Licensing

This element of the service leverages licensing.

Service Elements Scope

SCOPE ITEM	DESCRIPTION
Client Agreement	Creation of a Customer Agreement, between the client and Application, or OS Vendor
Manage licenses	Management of products and service subscription licenses
Billing Support	Provide billing support from application or OS vendor
Manage Tenant Subscription	Managed subscription changes on behalf of the Client
Reporting	Provide license total / usage
Invoicing	Invoice creation and delivery

Service Provision Excludes

EXCLUSION ITEM	DESCRIPTION
Installation of software	This element of service is described in SI: CO-ITSM-SD
Tracking of client licensing compliance	Client is responsible for maintaining licensing compliance on applications and OS

Service Requirements

REQUIREMENTS ITEM
N/A

Access Requirements

REQUIREMENTS ITEM
Access to customer licensing portal for application or OS vendor

Data Residency

RESIDENCY ITEM
N/A

Service Catalogue Request Items

CATALOG ITEM	FULFILMENT TIME	QUALIFYING CRITERIA	INCLUDED REQUESTS
Vendor or Application license Audit	40BHR	Client ticket submission for all applications and OS licenses	1 Monthly

License quote	40BHR	Provide quote of software licenses required as requested.	1 Weekly
---------------	-------	---	----------

Standard Reporting

REPORTING ITEM	DESCRIPTION	FREQUENCY
License Consumption report	Report of current license(s) purchase	1 Monthly

RACI Table

SERVICE ACTIVITIES	Calligo	Customer
Create a valid Customer Agreement between Application or OS vendor and Client	R, A	I
Accurate count of licenses required	A	R
Request changes to subscription being managed	I	R, A
Provide subscription billing invoices for managed subscriptions	R, A	I
Payment of subscription invoices from Calligo	I	R, A

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

13.5 BaaS – Office 365

This element of the service leverages backup tooling to provide M365 User Level Backups.

Service Elements Scope

SCOPE ITEM	DESCRIPTION
Mailbox Backup (Exchange Online)	Copy of all user's mailboxes including archive mailboxes and shared mailboxes
SharePoint Backup	Copy of all SharePoint data including custom web parts.
Teams	Copy of all Teams Sites, including team chat data and files shared within Teams
OneDrive Backup	Copy of any OneDrive for Business.
Storage	Up to 30GB per User Account. Additional storage above 30GB available at an additional cost.

Service Provision Excludes

EXCLUSION ITEM	DESCRIPTION
Unlicensed users	Service is unable to backup unlicensed users.
Project Web Apps	Not supported.
Microsoft Teams data	<p>Current exclusions for Teams:</p> <ul style="list-style-type: none"> • Private and shared channels • One-on-one and group chats • Audio and video calls • Video recordings saved to Microsoft Stream • Contacts • Code snippets in posts <p>Data of applications added as channel tabs (such as Website, Planner, Word, Excel, PowerPoint, Visio, PDF, Document Library, OneNote, SharePoint, Stream, Forms, Power BI, Power Automate and Azure DevOps) and other 3rd party</p>

	applications if their data does not reside in the SharePoint document library of the team
OneNote	Backups for OneNote, if size is more than 2 GB is currently not supported.
Storage	Storage requirements above 30GB unless previously agreed and provisioned at an additional cost.

Service Requirements

REQUIREMENTS ITEM
N/A

Access Requirements

REQUIREMENTS ITEM
For initial configuration of the service an account with the Global Admin role is required, after install and setup the accounts permissions can be updated to have the roles listed below.
Service Account (Standard Calligo Naming Convention) with the following roles for SharePoint (SharePoint Admin, View-only Configuration & View-Only Recipients) for Teams (Team Administrator)
Service Account requires a license with access to the Teams API (Minimum Microsoft Teams Exploratory experience)

Data Residency

RESIDENCY ITEM	DESCRIPTION	SYSTEM	STORAGE LOCATION
Backup for Microsoft 365	Location of the backup server and Storage location	Calligo Hosted	Dublin, IE Barrie, CA

Service Catalogue Request Items

CATALOG ITEM	FULFILMENT TIME	QUALIFYING CRITERIA	INCLUDED REQUESTS
Add or remove a user from the scope	24BHR	users may be added or removed from the scope. Must be raised as a ticket in Viaje	1 weekly
Changes to the retention policy	24BHR	Must be raised as a ticket in Viaje	1 monthly
Restore request	8BHR	Must be raised as a ticket in Viaje	As required

Standard Reporting

REPORTING ITEM	DESCRIPTION	FREQUENCY
Client Storage Usage	As Required	On Request
Client License Usage	As Required	On Request

Supporting Documentation and Details

Policy Name	Total Retention Period
Policy 1	1 Year

Policy 2	2 Year
Policy 3	3 Year
Policy 4	Keep Forever

RACI Table

SERVICE ACTIVITIES	Calligo	Customer
Backup Retention Specification	C	R, A
Backup Retention Configuration	R, A	C
Request to add or remove a user from the scope	C	R, A
Management of users	R, A	C
Backup Checks	R, A	I
Restore Test	R, A	I

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

13.6 Service Delivery Manager

This element of the service leverages an experienced Calligo Service Delivery Manager to assist with service management requests, reporting, escalations and technical advice and guidance as needed.

Service Element Scope

SCOPE ITEM	DESCRIPTION
Service Review Meetings	Regular meetings between the key stakeholders for the client and Calligo Service Delivery Managers to review an agreed set agenda, including Service Performance, Project Updates, Calligo Company Updates.
Service Reporting	Regular reports covering support ticket summary and performance against Service Levels, Availability and Capacity management (where applicable), Operations Management performance against Service Level Objectives.
Technical guidance	Access to business hours technical guidance and support to ensure customer's success, bringing Calligo's best ideas, standards, innovations, and capabilities to customers to drive maximum business value. Educate Calligo clients on how existing and new product features and functionality work, and how it can contribute to their business growth
Escalation contact	Calligo point of contact during Business hours for support requests and accounts escalations.

Service Provision Excludes

EXCLUSION ITEM	DESCRIPTION
24/7	Access to Service Delivery Managers is during business hours only.

Service Requirements

REQUIREMENTS ITEM
All support tickets are logged via the Calligo ITSM system by clients.
All Service Review reports are generated via Calligo Reporting dashboards
Access to client's key stakeholders and decision makers

Access Requirements

ACCESS REQUIREMENTS
N/A

Data Residency

RESIDENCY ITEM	DESCRIPTION	SYSTEM	STORAGE LOCATION
ITSM Data	ITSM Ticket information and logged attachments	Viaje	London Luxembourg Jersey

Service Catalogue Request Items

CATALOG ITEM	FULFILMENT TIME	QUALIFYING CRITERIA	INCLUDED REQUESTS
Review Meetings	1 Week	No previous review in past month	

Standard Reporting

REPORTING ITEM	DESCRIPTION	FREQUENCY
Service Review Reports	Covering support ticket summary and performance against Service Levels, Availability and Capacity management (where applicable), Operations Management performance against Service Level Objectives.	Monthly generated
Incident Reports	Providing Incident Reports for all major Incidents to outline the root cause and future mitigation to avoid reoccurrence.	For all P1 Incidents impacting the client

RACI Table

SERVICE ACTIVITIES	Calligo	Customer
Producing and delivering Service Reports	A, R	C, I
Scheduling and managing Service Review Meetings	A, R	C, I
Obtaining client feedback on Service levels	A, R	C, I
Providing feedback on Calligo Service levels	C, I	A, R
Providing management and oversight on active client projects	A, R	C, I
Delivery of Incident Reports and post incident review meetings	A, R	C, I
Approval for changes in service scope	C, I	A, R

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

13.7 Technical Account Manager

This element of the service leverages an experienced Calligo Technical Account Manager to assist with technical requests, reporting, escalations, and ongoing technical advice to help drive and direct client's strategy and need for information technology.

Service Elements Scope

SCOPE ITEM	DESCRIPTION
Service Review Meetings	Regular meetings between the key stakeholders for the client and Calligo to review an agreed set agenda, including Service Performance, Project Updates, Client IT Strategy roadmap, Calligo Company Updates.
Service Reporting	Regular reports covering support ticket summary and performance against Service Levels, Availability and Capacity management (where applicable), Operations Management performance against Service Level Objectives.
Technical guidance	Access to business hours technical guidance and support to ensure customer's success, bringing Calligo's best ideas, standards, innovations, and capabilities to customers to drive maximum business value. Educate Calligo clients on how existing and new product features and functionality work, and how it can contribute to their business growth.
Escalation contact	Calligo point of contact during Business hours for support requests and account escalations.

Service Provision Excludes

EXCLUSION ITEM	DESCRIPTION
24/7	Access to Technical Account Managers is during Business Hours only as specified in the MSA.
Implementation services	This service does not include activities that would be classified as development or project work.

Service Requirements

REQUIREMENTS ITEM
All support tickets are logged via the Calligo ITSM system by clients.

Access Requirements

REQUIREMENTS ITEM
Administrative access to all assets in scope as required for remediation actions

Data Residency

RESIDENCY ITEM	DESCRIPTION	SYSTEM	STORAGE LOCATION
ITSM Data	ITSM Ticket information and logged attachments	Viaje	London Luxembourg Jersey

Service Catalogue Request Items

CATALOG ITEM	FULFILMENT TIME	QUALIFYING CRITERIA	INCLUDED REQUESTS
--------------	-----------------	---------------------	-------------------

Not applicable			
----------------	--	--	--

Standard Reporting

REPORTING ITEM	DESCRIPTION	FREQUENCY
Incident Reports	Providing Incident Reports for all major Incidents to outline the root cause and future mitigation to avoid reoccurrence.	For all P1 Incidents impacting the client

RACI Table

SERVICE ACTIVITIES	Calligo	Customer
Producing and delivering Incident Reports and post incident review	A, R	I
Scheduling and managing technical roadmap Review Meetings	A, R	C, I
Obtaining client feedback on Service levels and Performance	A, R	C
Providing feedback on Calligo Service levels and Performance	I	A, R
Providing technical oversight on active client projects within scope	A, R	C, I
Approval for changes in service scope	C, I	A, R

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

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.