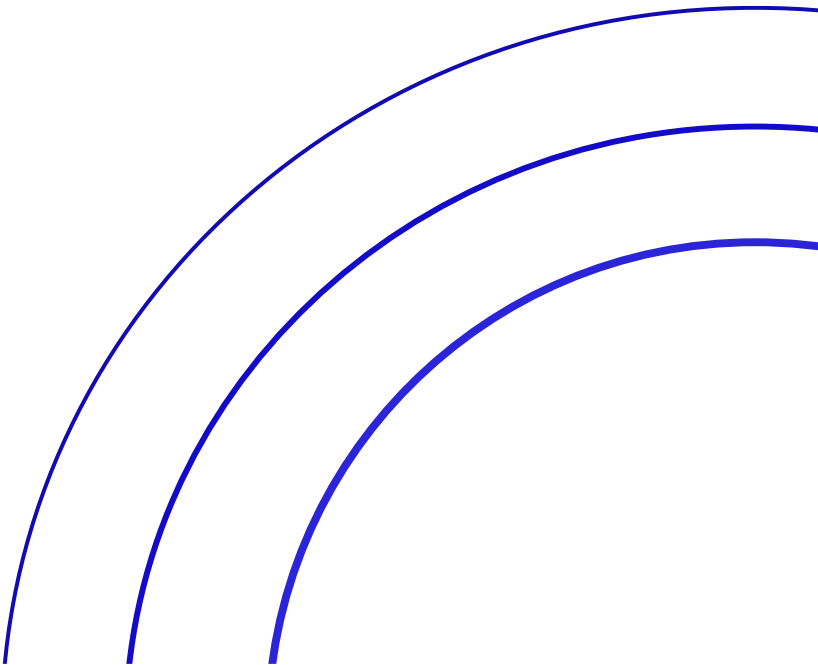
Managed Physical Server
Service Description



Document Control

TITLE:	**Managed Physical Server Service Description**	**DOCUMENT REF NO:**	QMS REC65
DESCRIPTION:	This document defines the services provided by Calligo's Managed Physical Server service		
OWNER/ AUTHORITY:	Director, Operations Management	**VERSION NO:**	1.10
DOCUMENT CROSS REFERENCE:	N/A	**VERSION DATE:**	06/10/2023
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, Calligo ("Entity") on 25 November 2022

CHANGE HISTORY RECORD				
VERSION	**DESCRIPTION OF CHANGE**	**AUTHOR**	**APPROVAL**	**DATE OF ISSUE**
1.0	Initial Issue	Director, Product & Service Development	CEO	30/10/17
1.1	Verbiage Review	Director, Product & Service Development	CEO	09/11/17
1.2	Added RACI Matrix, Glossary of Terms and amendments	Director, Product & Service Development	CEO	18/01/18
1.3	Verbiage Review	Director, Product & Service Development	Chief Experience Officer	26/01/18
1.4	Group Review	Legal Counsel	CISO	19/03/18
1.5	Verbiage Review	Legal Counsel	Director, Product & Service Development	09/08/19
1.6	Re-design, change of ownership and verbiage review	Director, Operations Management	VP, Cloud Operations	25/11/22
1.7	Remove Service Locations table and add link to external Service Locations document.	Director, Operations Management	VP, Cloud Operations	10/01/23
1.8	Updated supporting documentation links	Director, Operations Management	VP, Cloud Operations	20/02/23
1.9	Updated optional offerings	Director, Operations Management	VP, Cloud Operations	25/09/23
1.10	Updated optional offerings	Director, Operations Management	VP, Cloud Operations	05/10/23

2. Service Overview

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

Managed Physical Server is a managed Server 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. The service also includes Monitoring for, Heartbeat, Services and OS health as well as support for the on prem hardware layer.

3. Service Inclusions

3.1. CO-ITSM-OSP

This service leverages Datto RMM and PowerBI to deliver patching and reporting to Windows OS assets.

3.2. 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

3.3. CO-ITSM-MON

This service leverages Datto RMM and PowerBI to deliver monitoring and reporting for the in-scope service assets.

3.4. CO-ITSM-ONSITE

As required on-site support for in-scope hardware as defined by the required service item(s).

4. Service Provisions

4.1. CO-ITSM-OSP

4.1.1. Inclusions

CO-ITSM-OSP	
Scope Item	**Description**
Monthly patching of systems running Windows OS currently supported by Microsoft	For supported OS versions: Deprecated OS versions require a separate Microsoft Extended Support Contract and a separate deployment agreement. Applicable patches are automatically approved unless otherwise agreed via Patch Advisory reporting and additional approval workflows. Critical, Monthly and Security updates are included as part of regular patch deployments.
Configuration and maintenance of deployment rules, settings, and deployment options.	Administration of rules, products, update classifications, agent settings Zero-day patch deployment
Consolidation of Monthly updates into cumulative updates and deployment of the cumulative updates.	Previous months applicable patches are consolidated into a single deployment to cover all patches in all previous deployments. These deployments are active with the current months deployments and follow the same schedule.
Maintenance of groups for systems in scope	Checking health and heartbeat of assigned assets in specific groups and schedules.
Exclusion of patches from deployment scope for known	Removal of patches from deployment scope for known issues with the patch or as a result of testing during the pilot deployment.

issues with the patch or resulting from testing during the pilot deployment	
Standard Reporting	Standard Monthly and regularly scheduled reports are included in this service.

4.1.2. Exclusions

CO-ITSM-OPS	
Exclusion Item	**Description**
The development of patch “work arounds” in the absence of an approved system vendor’s patch.	This is a chargeable addition to the service and is priced on effort required as each mitigation or “work around” is unique.
Ad-hoc and /or custom patch reporting	This is a chargeable addition to the service and is priced on effort required.
Manual Patching of systems	This is a chargeable addition to the service and is priced on effort required.
Removal of patches from systems once installed	This is a chargeable addition to the service and is priced on effort required as backouts can vary and be unique.
Remediation or recovery of non-compliant systems caused due to existing OS issue.	The required patches are identified, downloaded and the installation is attempted but fails due to OS issues. Any troubleshooting beyond included remediation steps is a chargeable addition to the service. If the server blue screens due to applied patches during or immediately after patch installation, any troubleshooting beyond included remediation steps is a chargeable addition to the service.
Performing manual vulnerability remediation steps.	Manual steps required before or after automated patching windows is a chargeable addition to the service and is priced on effort required. This falls into the same area as “Manual patching of systems” above.
Compliance on assets added/removed without notification, or where configuration changes have been made to assets without submission via Change Management Process	Calligo needs to be informed in the form of a change record to the scope or configuration changes that could impact agent's health and the patching process.

4.2. CO-ITSM-SD

4.2.1. 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.

4.2.2. 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.

4.3. CO-ITSM-MON

4.3.1. Inclusions

CO-ITSM-MON	
Scope Item	**Description**
Base OS Monitoring	Monitoring covers in-support Windows Server family operating systems
Resource Monitoring	The following items are currently within scope -CPU utilization -Memory (RAM) utilization -Disk utilization
Availability Monitoring	-RMM Agent heartbeat -URL availability
Remediation	-Remediation services to ensure all management functionality is operable -Remediation services to restore operability, or resolve service availability issues of monitored options
Service Monitoring	Monitoring of core OS and role services (defined as per service design)

4.3.2. Exclusions

CO-ITSM-MON	
Exclusion Item	**Description**
End-of-Life OS	Microsoft OS that has passed end of support date and no extended support agreement exists
End user OS	Non-Windows Server OSes (e.g., Windows 10)
Non-OS application	3rd party software installed to a monitored system Troubleshooting of issues at the application level for applications related to services not provided by Calligo.
Licensing	Application or Server licensing expiration or renewal periods
Customer Internet Connectivity	Monitoring of external IP addresses for connectivity
Procurement	As part of remediation activities, procurement of required hardware or software is out of scope and requires a separate service agreement
Specific Functionality	Monitoring can detect if a system or service is available, but cannot validate full functionality

4.4. CO-ITSM-ONSITE

4.4.1. Inclusions

CO-ITSM-ONSITE	
Scope Item	**Description**
Supported Hardware	• Servers • Routers • Firewall Appliances • Switches • Workstations • Printers
Onsite travel to client location to facilitate repair	A service technician will be dispatched to client site to assess and initiate repair or replacement of failed components.
Removal of equipment for offsite repair	In the event repair cannot be facilitated on onsite, it may be required to remove equipment and transport it to either a Calligo repair facility or third party / vendor repair facility. This will require the Equipment Removal Procedure to be followed.

4.4.2. Exclusions

CO-ITSM-ONSITE	
Exclusion Item	**Description**

Upgrades of hardware beyond original specifications	Unless original replacement components are unavailable and have been replaced with newer versions / revisions, original replacement components will be used.
Reconfiguration or equipment	Equipment will be repaired and restored to original order and functionality prior to fault.
Unsupported Hardware	• Power Distribution Units • UPS

5. Roles and Responsibilities

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

Service Activities – Core Elements	Calligo	Customer
CO-ITSM-OSP		
Business application verification, maintenance, and testing	C, I	R, A
Patch Deployment	R, A, C	
Defining standard recurring deployment schedules, exclusions, and targets	C, I	R, A
Compliance measurement for SLO/SLA purposes	R, A, C	I
Maintenance of SCEM collections for systems in scope	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
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
Provide SMTP relay for subscription-based delivery of reports and alerts	C, I	R, A
Run reports on a scheduled basis and provide malware detection alerts	R, A	C, I
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
Provide SMTP relay for subscription-based delivery of reports and alerts	C, I	R, A
Run reports on a scheduled basis and provide malware detection alerts	R, A	C, I
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
CO-ITSM-MON		
Configuring standard monitoring	R, A	C, I
Requesting monitoring changes	R, C	R, A
Responding to alerts	R, A	C, I
Remediation	R	R, I
CO-ITSM-ONSITE		
Facilitate support with Third Party suppliers for issues with their products or services that are in scope of support including arranging replacement components.	R, A	C
Maintain valid support contracts for third party suppliers	I	R, A

Allow Calligo to act as an agent for support of Third-Party products or services	C	R, A
Installation, configuration, upgrade of Third-Party applications and services not related to hardware servicing.	C, I	R, A

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

6. Reporting

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

Service Item	Reporting Item	Description	Frequency
CO-ITSM-OSP	**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-OSP	**Patch Advisory**	The report lists all required patches that are scheduled for deployment.	1 Monthly. Sent a day after Patch Tuesday
CO-ITSM-OSP	**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-OSP	**Asset Compliance State (Current Cycle)**	Current patch compliance state for the current month deployments.	1 Monthly after deployment completion
CO-ITSM-OSP	**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
CO-ITSM-MON	**Monitoring Performance**	Average values of resource utilization for monitored systems during the previous period	Monthly
CO-ITSM-MON	**Monitoring Alerts**	Alerts raised during the previous period and current status (open or resolved)	Monthly
CO-ITSM-MON	**Device Monitor status**	List of configured monitors for each supported system	Monthly

7. Data Residency

Calligo Data Residency

8. Service Requirements

Service Item	Requirements Item
CO-ITSM-OSP	Current in support or Extended support Windows OS assets.
CO-ITSM-OSP	Deployment of Datto RMM agent and relevant firewall / access configurations for each in scope asset
CO-ITSM-OSP	An agreed and defined re-occurring maintenance window for automated patch installation and remediation activities
CO-ITSM-OSP	Reboots are permitted within the agreed maintenance windows.
CO-ITSM-OSP	Outbound internet access for monitoring 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.
CO-ITSM-MON	Datto RMM Agent must be installed to all monitored assets
CO-ITSM-MON	Network connectivity and necessary access rules are required for all monitored assets

9. 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

10. Support Locations

Calligo Support Locations

Location Item	Description	Location
Service Desk	Calligo Service Desk (L1 to L3)	UK, Ireland, Channel Island, Canada
Operations Centre	Calligo Network Operations Centre	Sri Lanka, Canada
Operations Management	Calligo Operations Management Team	UK, Canada, Sri Lanka

11. Service Catalogue Request Items

Catalogue Item	Fulfilment Time	Qualifying Criteria	Included Requests
Add/Remove asset from scope	8BHR	Supplied list of assets	1 per week
Modify Patch categories	24BHR	Supplied list of categories to modify and required changes.	1 per week
On demand tracking of compliance states	1BHR	Specific KB patch tracking submission	1 Monthly
Monitoring Report	48BHR	Provides data available from the platform	1 per week
Additional service monitoring	48BHR	Additional monitors may be added to existing systems	1 per week
Modify alert recipients	48BHR	Alert recipients may be adjusted to include client stakeholders	1 per week
Modify alert thresholds	48BHR	Client may request custom thresholds for an alert to be raised	1 per week
On demand tracking of compliance states	1BHR	Specific KB patch tracking submission	1 Monthly

12. Standard SLO's

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

13. 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

14. Optional Services

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

14.1. Anti-Virus - Endpoints

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 or receive timely updates/policies and protection.

Access Requirements

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

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

14.2. M365 Applications

Service Elements Scope

This element of the service leverages Microsoft 365 applications and tooling for end user configuration.

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
(M365 Application Patching Tooling) Monthly patching of systems running in scope Office applications currently supported by Microsoft	For supported OS versions: Deprecated OS versions require a separate Microsoft Extended Support Contract and a separate deployment agreement. Applicable patches are automatically approved unless otherwise agreed via Patch Advisory reporting and additional approval workflows. Critical, Monthly and Security updates are included as part of regular patch deployments.
(M365 Application Patching Tooling) Configuration and maintenance of deployment rules, settings, and deployment options.	Administration of rules, products, update classifications, agent settings Zero-day patch deployment
(M365 Application Patching Tooling) Consolidation of Monthly updates into cumulative updates and deployment of the cumulative updates.	Previous months applicable patches are consolidated into a single deployment to cover all patches in all previous deployments. These deployments are active with the current months deployments and follow the same schedule.
(M365 Application Patching Tooling) Maintenance of groups for systems in scope	Checking health and heartbeat of assigned assets in specific groups and schedules.

SCOPE ITEM	DESCRIPTION
(M365 Application Patching Tooling) Exclusion of patches from deployment scope for known issues with the patch or resulting from testing during the pilot deployment	Removal of patches from deployment scope for known issues with the patch or as a result of testing during the pilot deployment.
(M365 Application Patching Tooling) Standard Reporting	Standard Monthly and regularly scheduled reports are included in this service.
(M365 Application Patching Update Channel)	Configuration of update channels: • Current Channel • Monthly Enterprise Channel • Semi-Annual Enterprise Channel • Semi-Annual Enterprise Channel (Preview)

Service Provision Excludes

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
The development of patch “work arounds” in the absence of an approved system vendor’s patch.	This is a chargeable addition to the service and is priced on effort required as each mitigation or “work around” is unique.
Ad-hoc and /or custom patch reporting	This is a chargeable addition to the service and is priced on effort required.
Manual Patching of systems	This is a chargeable addition to the service and is priced on effort required.
Removal of patches from systems once installed	This is a chargeable addition to the service and is priced on effort required as backouts can vary and be unique.
Remediation or recovery of non-compliant systems caused due to existing OS issue.	The required patches are identified, downloaded and the installation is attempted but fails due to OS issues. Any troubleshooting beyond included remediation steps is a chargeable addition to the service. If the server blue screens due to applied patches during or immediately after patch installation, any troubleshooting beyond included remediation steps is a chargeable addition to the service.
Performing manual vulnerability remediation steps.	Manual steps required before or after automated patching windows is a chargeable addition to the service and is priced on effort required. This falls into the same area as “Manual patching of systems” above.
(M365 Application Patching Update Channel) Standard Reporting	Currently there is no supported reporting export for version compliance. Dashboard visual is the only representation. *Note: This item will be revisited on a regular basis for improvements to this service element.*

Service Requirements

REQUIREMENTS ITEM
All applicable M365 licenses Current in support or extended support Windows OS assets. Deployment of Datto RMM agent and relevant firewall / access configurations for each in scope asset An agreed and defined re-occurring maintenance window for automated patch installation and remediation activities Reboots are permitted within the agreed maintenance windows. Outbound internet access for reporting and patching.

Access Requirements

REQUIREMENTS ITEM
Administrative (Local) access to all assets in scope as required.
Required Administrative rights to client M365 Tenant.
Service Account for Datto RMM agent activities

Service Catalog Request Items

This table represents the items and frequency that can be requested during the service cycle.
Note: Additional requests are chargeable and are priced on effort required.

CATALOG 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

Standard Reporting

This table represents the standard reports included in **CO-ITSM-M365APP** as well as the deliverable frequency.

REPORTING ITEM	DESCRIPTION	FREQUENCY
M365 usage	Mailbox sizing, OneDrive sizing and assigned licenses.	1 Monthly
OneDrive External Sharing	Lists of current external OneDrive shares	1 Monthly
Security and Compliance reporting	Office 365 Secure Score, DLP Policy	1 Monthly
(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
(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
(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.
(M365 Application Patching Tooling) Asset Compliance State (Current Cycle)	Current patch compliance state for the current month deployments.	1 Monthly after deployment completion
(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

RACI Table

SERVICE ACTIVITIES	Calligo	Customer
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

SERVICE ACTIVITIES	Calligo	Customer
(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
Run reports on a scheduled basis and provide malware detection alerts	R, A	C, I

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

14.3. Application Currency

Service Elements Scope

This element of the service leverages tooling to provide updates to existing deployed supported applications.

SCOPE ITEM	DESCRIPTION
Monthly patching of Applications in scope for third-party updates	For supported OS versions: Windows 7 and above. Windows 7 requires a separate Microsoft Extended Support Contract. Third-party applications are patched using vendors catalogues or third-party tools
Administration of Third-party catalogues, products, update classifications, agent settings	Configuration and maintenance of third-party update catalogues, deployment rules, Datto agent settings and deployment options.
Installation and configuration of Third-party update tools or add-ons	If required, third-party update tools or add-ons will be installed and configured to provide application currency
Service Catalog Items	A standard list of requestable items included in this service.

Service Provision Excludes

EXCLUSION ITEM	DESCRIPTION
Updates for Applications not available by 3rd party tools or add-ons	This is a chargeable addition to the service and is priced on effort required. These applications are updated using Application deployment and package creation.
Manual patching of systems	This is a chargeable addition to the service and is priced on effort required. These applications are updated using Application deployment and package creation.

Service Requirements

REQUIREMENTS ITEM

Datto RMM agent installed on all in scope assets.
CO-ITSM-OPS, Workstation OS Patching is required as the configuration and deployments are utilized as core functionality.
Third-party update tools or add-ons, if needed

Access Requirements

REQUIREMENTS ITEM
Datto RMM agent installed on all in scope assets
Local Administrator access to all systems in scope is required for troubleshooting and remediation actions.

Service Catalogue Items

This table represents the items and frequency that can be requested during the service cycle.
Requests are chargeable and are priced on effort required.

CATALOG ITEM	FULFILMENT TIME	QUALIFYING CRITERIA	INCLUDED REQUESTS
On demand tracking of compliance states	8BHR	Specific KB patch tracking submission	1 Monthly
Request for not supported applications to Catalog	24BHR	Submitted application required and may not be supportable upon investigation.	1 Weekly

Standard Reporting

REPORTING ITEM	DESCRIPTION	FREQUENCY
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
Patch Advisory	The report lists all required patches that are scheduled for deployment.	1 Monthly. Sent a day after Patch Tuesday
Pre-Patch Compliance Report	The report includes compliance summary and a list of non-compliant systems.	1 per deployment. Sent prior to deployment.
Asset Compliance State (Current Cycle)	Current patch compliance state for the current month deployments.	1 Monthly after deployment completion
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

RACI Table

SERVICE ACTIVITIES	Calligo	Customer
Business application verification, maintenance, and testing	C, I	R, A
Patch Deployment	R, A, C	-
Defining standard recurring deployment schedules, exclusions, and targets	C, I	R, A
Compliance measurement for SLO/SLA purposes	R, A, C	I
Maintenance of Datto collections for systems in scope	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
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
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
Submission requests for additional, not currently supported applications	R, C	A, I

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

14.4. M365 Identity and Access Management

Service Elements Scope

This element of the service leverages Microsoft Active Directory and Microsoft Azure Active Directory.

SCOPE ITEM	DESCRIPTION
(AD) Manage and maintain the Active Directory infrastructure solution	Ensures the availability of Active Directory identity services and replication across sites

(AD) User and group creation, modification and removal	Management of users and groups (including group membership) for role-based access
(AD) Group Policy creation	Management of system and user policies governing functionality
(AD) Active Directory Domains and Trust management	Management of AD forests
(AD) Authorize DHCP Servers in Active Directory	Authorize Windows-based DHCP servers to operate within the network
(AD) DNS Server management	Management of DNS zones
(AD) Remediation	Remediation of Active Directory replication failures
(AAD) User and group creation, modification, and removal	Management of users and groups
(AAD) Delegation of security privileges within Azure Active Directory	Management of user and group rights to AAD management functions
(AAD) Delegation of Role Based Access Control (RBAC) roles for specific Microsoft applications	Management of user and group rights to Microsoft applications
(AAD) Publishing of gallery-based applications	Publishing of native Azure AD applications
(AAD) Basic application portal branding	Branding of the Microsoft 365 sign-in portal
(AAD) Self-service password reset configuration	Implementation of SSPR to permit users to reset a forgotten password independently

Service Provision Excludes

This table represents any exclusions to the services provided.

EXCLUSION ITEM	DESCRIPTION
(AD) End-of-Life OS	Microsoft OS's that have passed end of support date and no extended support agreement exists
(AD) Inter-site connectivity	Availability of network routes and connectivity between sites
(AAD) Custom gallery applications	Azure applications not published to the gallery

Service Requirements

This table represents the items required for this service.

REQUIREMENTS ITEM
(AAD) Azure AD Premium P2 OR EM+S E5 OR M365 E5 (AD) Current Windows Server OS within manufacturer's support period

Access Requirements

This table represents the items required for this service.

REQUIREMENTS ITEM
(AD) Domain admin rights are required to manage Active Directory
(AAD) Global admin rights are required to manage Azure Active Directory

Service Catalog Request Items

This table represents the items and frequency that can be requested during the service cycle.
Note: Additional requests are chargeable and are priced on effort required.

CATALOG ITEM	FULFILMENT TIME	QUALIFYING CRITERIA	INCLUDED REQUESTS
Create New User	24BHR	User's name, access rights, start date	5 per week
Disable User	8BHR	User's name, effective date	5 per week
Create/Update/Delete Group	24BHR	Group name, members	5 per week
Group policy management	24BHR	Policy requirements, user/machine scope	3 per week
Domain Trust	48BHR	Incoming domain name, trust type, target domain service account	1 per month
DNS record or zone modification	16BHR	Zone name, record type, data (IP or string)	1 per week
(AAD) Role-Based Access Control Grant/Deny	16BHR	User account, access role	5 per week
(AAD) Publish gallery application	16BHR	Application name and applicable configurations	1 per week

Standard Reporting

This table represents the standard reports included in **CO-ITSM-IDENT** as well as the deliverable frequency.

REPORTING ITEM	DESCRIPTION	FREQUENCY
User report	User Canonical Name, group memberships, account name (UPN and sAMAccountName), password expiry, account status, etc.	Monthly
(AAD) Access history	Account sign-ins	Monthly
(AAD) Activity Reports	User activity logs	Monthly
(AD) File Share Report	File shares and permissions	Monthly

RACI Table

The RACI Table provides a responsibility matrix for the in-scope AD and AAD Identity Management activities.

SERVICE ACTIVITIES	Calligo	Customer
User access changes (grant/deny)	R, A, C	R, C
Support for 3rd Party Applications	I	R, A, C
Provisioning of Licenses (User and Server)	I	R, A, C
Approving Privileged Access	C, I	R, A
Management of Computer Object Lifecycle	C, I	R, A
Establishing Trusts to Other Domains	R, A	R, A

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

14.5. 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

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

14.6. 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 backups unlicensed users.
Project Web Apps	Not supported.
Microsoft Teams data	Current exclusions for Teams: • 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 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 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)

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

14.7. 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

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

14.8. 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

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

15. Auxiliary Services

15.1. Service Onboarding & Transition

To launch Managed Physical Server 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 Physical Server 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.

15.2. 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.

15.3. 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.