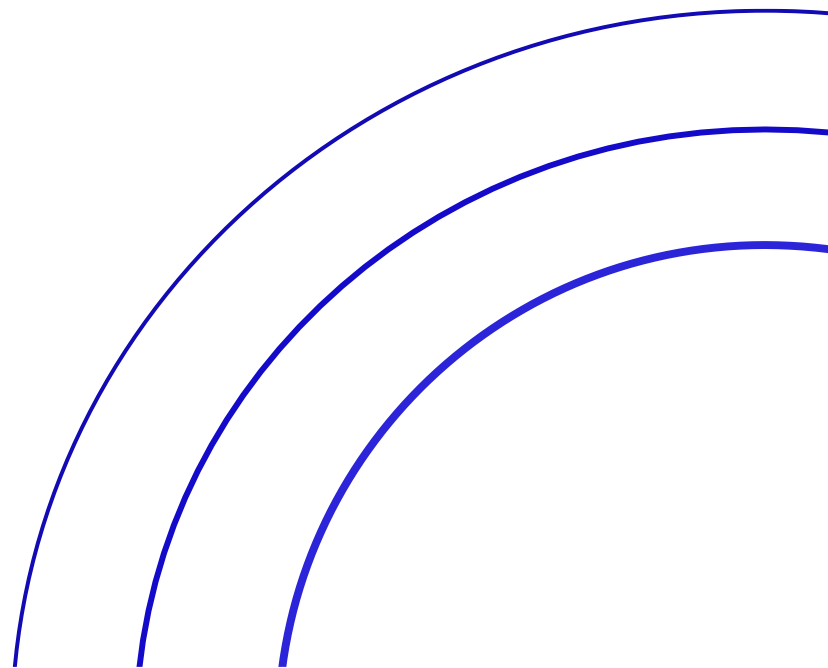**Managed Virtual Desktop
Service Description**

Document Control

TITLE:	Managed Virtual Desktop Service Description	DOCUMENT REF NO:	QMS REC107
DESCRIPTION:	This document defines the services provided by Calligo's Managed Virtual Desktop service		
OWNER/ AUTHORITY:	Director, Operations Management	VERSION NO:	1.2
DOCUMENT CROSS REFERENCE:	N/A	VERSION DATE:	20/02/2023
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	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	Updated supporting documentation links	Director, Operations Management	VP, Cloud Operations	20/02/23

1. Service Overview

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

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

2. Service Inclusions

1.1. CO-ITSM-OSP

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

1.2. 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

1.3. CO-ITSM-MON

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

3. Service Provisions

1.4. CO-ITSM-OSP

1.4.1. 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 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.
Standard Reporting	Standard Monthly and regularly scheduled reports are included in this service.

1.4.2. 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.

1.5. CO-ITSM-SD

1.5.1. 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.

1.5.2. 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.

1.6. CO-ITSM-MON

1.6.1. 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)

1.6.2. 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. Roles and Responsibilities

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

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

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

5. Reporting

The table below provides details on the additional Monthly Reporting and Analytics for Managed Virtual Desktop 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

6. Data Residency

Calligo Data Residency

7. 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

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

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

10. 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

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 to the Managed Virtual Desktop service, Calligo can provide the following service items as optional add on services for Managed Virtual Desktop:

Service Item	Service Item Reference	Description
M365 Threat Protection	CO-ITMS-M365TP	Calligo's M365 Threat protection provides endpoint level Antivirus and Malware protection.
M365 Applications	CO-ITSM-M365APP	Calligo's M365 Application support provides real time monitoring of the M365 Tenant as well as User management and Mailbox provisioning. Technical support is provided for Word, Excel, PowerPoint, Teams, Outlook, OneDrive and SharePoint Online.
Application Currency	CO-ITSM-ACAAS	Calligo's Application Currency as a Service adds and additional layer of patch currency and security to installed third party applications.
Licensing	CO-SW-LICENCE	Calligo's Licencing Service provides Application, OS and Appliance licensing procurement as well as Provisioning and Management of service subscriptions. Reporting of license usage as well as monthly Invoicing provides detailed status of all current client licensing.
365 User Protected User	CO-BAAS-365USER	Calligo's M365 Application and data level backups provides data assurance for all supported M365 applications.
Service Delivery Manager	CO-ITSM-SDM	The Service Delivery Manager will be responsible for the business as usual and account management relationship. This will include service reviews, point of escalation, responsible for Information Technology Infrastructure Library (ITIL) practice adherence, interfacing with third-party suppliers also participating under the customer's Service Integration and Management model and ensuring that Calligo meets or exceeds Service Level Objective (SLO) targets.
Technical Account Manager	CO-ITSM-TAM	The Technical Account Manager will be responsible for the technical collaboration between the customer and Calligo support teams and will play a key role in technical service improvement, managing deployment of new services or configuration changes, ensuring optimal performance and uptime of the application stack, and interfacing with third-party suppliers as required under the customer's support model.

14. Auxiliary Services

1.7. Service Onboarding & Transition

To launch Managed Virtual Desktop 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 Virtual Desktop 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.

1.8. 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.

1.9. 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.