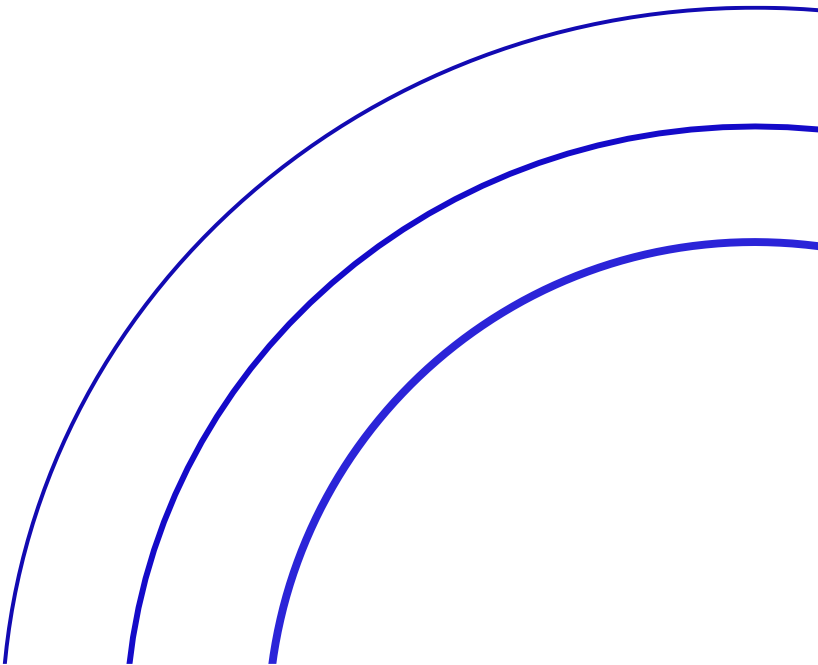
DRaaS Service Description



Document Control

TITLE:	**DRaaS Service Description**	**DOCUMENT REF NO:**	QMS REC62
DESCRIPTION:	This document defines the services provided by Calligo's DRaaS service.		
OWNER/ AUTHORITY:	VP, Cloud Operations	**VERSION NO:**	1.7
DOCUMENT CROSS REFERENCE:	N/A	**VERSION DATE:**	25/11/2022
DISTRIBUTION METHOD	Email and Website	**DOCUMENT CLASSIFICATION**	Internal

DOCUMENT OWNER & APPROVAL
The VP Cloud Operations 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 Chief Operating Officer, 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	04/12/17
1.3	Verbiage Review	Director, Product & Service Development	Chief Experience Officer	06/01/18
1.4	Group Review	Legal Counsel	CISO	05/03/18
1.5	Verbiage Review	Legal Counsel	Director, Product & Service Development	09/08/19
1.6	Re-design, change of ownership and verbiage review	VP, Cloud Operations	Chief Operating Officer	25/11/22
1.7	Remove Service Locations table and add link to external Service Locations document.	Director, Operations Management	Chief Operating Officer	10/01/23

1. Service Overview

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

Calligo's DRaaS (CloudShield) is designed to maintain business continuity and minimise data loss 24/7 without the need to invest in "always-on" hardware.

Designed to replicate virtual, physical and cloud hosted servers to Calligo's hosted servers between Calligo datacentre regions, IT workloads are automatically replicated in real time providing continuous data protection (CDP) with the ability to perform point in time recovery.

Calligo will manage the failover of protected critical systems as defined by the client in the event of a failure and restore services within agreed service levels to meet business continuity objectives.

2. Service Inclusions

2.1. CO-CC-DRAAS

This service is designed to replicate virtual, physical and cloud hosted servers to Calligo's hosted servers between Calligo datacentre regions, IT workloads are automatically replicated in real time providing continuous data protection (CDP) with the ability to perform point in time recovery.

2.2. 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

2.3. CO-ITSM-MON

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

3. Service Provisions

3.1. CO-CC-DRAAS

3.1.1. Inclusions

CO-CC-DRAAS	
Scope Item	**Description**
Specification	Specification of compute, networking, and storage requirements
Configuration	Configuration of compute, networking, and storage requirements Configuration and management of Calligo-side CloudShield components
Monitoring	This element of service is described in SI: **CO-ITSM-MON**
DR Run Book	Maintenance of the DR Runbook
Reporting	Produce quarterly reports confirming health and status of DR replication for compliance purposes
Testing	Responsibility for testing DR procedures executed successfully

3.1.2. Exclusions

CO-CC-DRAAS	
Exclusion Item	**Description**
Windows File System Backups	System file/directory exclusions: **\Winsxs* **\Pagefile.sys **\SoftwareDistribution* Locked files (files that are locked by applications or system programs while they are in use) are backed up using snapshots.
Removable Media	Any removable media attached to the VM will not be included in the backup jobs.

3.2. CO-ITSM-SD

3.2.1. 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.

3.2.2. 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.

3.3. CO-ITSM-MON

3.3.1. 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)

3.3.2. 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. Roles and Responsibilities

The table below provides a responsibility matrix for the core DRaaSelements:

Service Activities – Core Elements	Calligo	Customer
CO-CC-DRAAS		
Specification of compute, networking, and storage requirements	A, R	C
Configuration of compute, networking, and storage requirements	A, R	C
Monitoring and management of replication status	A, R	C
Maintenance of DR Runbook	A, R	C
Decision to invoke DR	C	A, R
Invoke DR procedures and failover services to secondary site	A, C	R
Invoke DR procedures and failback services to primary site	A, R	C, I
Ensure that changes related to VMs required for protection are requested	C, I	A, R
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 DRaaS that are included in the core service:

Service Item	Reporting Item	Description	Frequency

CO-CC-DRAAS	DR Health Status	Report confirming health and status of DR replication for compliance purposes	Based on schedule of service management reporting
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-CC-DRAAS	Client is responsible for ensuring that any application that does continuous writing such as backups are not included in protected VMs
CO-CC-DRAAS	Client is responsible for the protection of any VMs, or data not covered under CloudShield that will be required on the destination site
CO-CC-DRAAS	Client will define servers to be protected
CO-CC-DRAAS	Optional requirement of backup and restore is available as required. SI: **CO-CC-BAAS**
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
Service Account with access to the client's file system. (This is a requirement for file level recovery.)
Administrative access to all assets in scope as required for remediation actions
The Client agrees to maintain a permanent, dedicated Internet connection with sufficient bandwidth to enable Calligo to deliver this service within agreed SLO's. Bandwidth requirements will increase with amount of data protected and change rate.
Clients can have multiple levels of access providing an increased level of control and adherence to governance. • User – View the Disaster Recovery service status for Virtual Machines Administrator – As per User plus, Manager Disaster Recovery service for Virtual Machines such as failover

9. Support Locations

Calligo Support Locations

10. Service Catalogue Request Items

Catalogue Item	Fulfilment Time	Qualifying Criteria	Included Requests
Add or remove a system from the scope	24BHR	Systems may be added or removed from the scope. Must be raised as a Service Request	1 weekly
Changes to the retention policy	24BHR	Must be raised as a Service Request	1 monthly
Restore request	8BHR	Must be raised as a Service Request	As required
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
Additional DR execution	1 Business week	None in previous 3 months	4 times per year

11. Standard SLO's

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

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

12. Optional Services

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

Service Item	Service Item Reference	Description
CloudCopy (BaaS)	CO-CC-BAAS	Calligo's Backup as a Service is a managed service that is designed to remove the overhead and complexity of managing and restoring data, irrespective of where the data resides. By establishing a secure connection to Calligo's hosted infrastructures, data can be safely and securely backed up and stored in encrypted format to protect the integrity of the data.
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.

13. Auxiliary Services

13.1. Service Onboarding & Transition

To launch DRaaS 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 DRaaS 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.

13.2. 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.