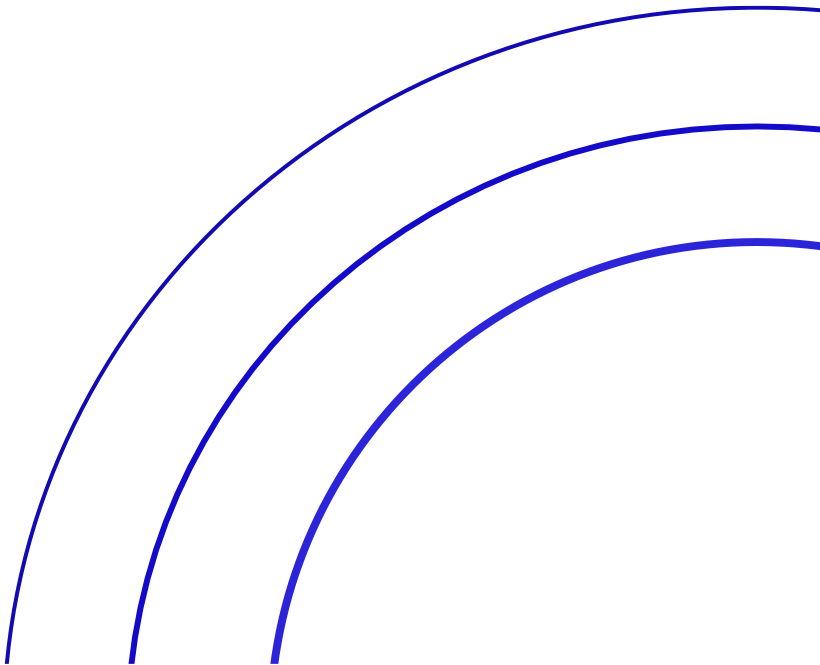
Calligo

BaaS Service Description



Document Control

TITLE:	**BaaS Service Description**	**DOCUMENT REF NO:**	QMS REC51
DESCRIPTION:	This document defines the services provided by Calligo's BaaS service		
OWNER/ AUTHORITY:	VP, Cloud Operations	**VERSION NO:**	1.7
DOCUMENT CROSS REFERENCE:	N/A	**VERSION DATE:**	23/11/2022
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 23 November 2022

CHANGE HISTORY RECORD				
VERSION	**DESCRIPTION OF CHANGE**	**AUTHOR**	**APPROVAL**	**DATE OF ISSUE**
1.0	Initial Issue	Director, Product & Service Development	CEO	17/10/17
1.1	Verbiage Review	Director, Product & Service Development	CEO	06/11/17
1.2	Added RACI Matrix, Glossary of Terms and amendments	Director, Product & Service Development	CEO	01/12/17
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	General 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	23/11/22
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 BaaS service. The BaaS service is one of a suite of services within the Calligo Operating Model.

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.

The Client is responsible for defining its own backup and retention schedules to meet its specific business or regulatory requirements.

2. Service Inclusions

2.1. CO-CC-BAAS

This service provides a multi-tenant solution for providing backup as a service, this service can provide VM level backups and application-aware backups.

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

3. Service Provisions

3.1. CO-CC-BAAS

3.1.1. Inclusions

CO-CC-BAAS	
Scope Item	**Description**
VM Level Backups	CommVault takes a copy of all the VM Data from vCenter by default this includes all virtual disks attached to the VM and copies the vCenter Configuration (Network, CPU & Memory)
Application-Level Backups	SQL: This captures the SQL Databases in a consistent state, these backups can be restored in place or out of place directly into an SQL server without having to restore the entire server. Windows File System: This is an indexed file level backup this can be used to take backups of shared folders/Drives without having to backup entire VMs, this can allow more regular backups of data.
Backup Checks	The Network Operations Center receive daily backup reports from CloudCopy, and any issues are resolved or escalated to the required team for investigation.
Restore Testing	The Network Operations Center completed a File Level and VM Level restore monthly in each region (this is not per customer and the data to restore is selected at random monthly).

3.1.2. Exclusions

CO-CC-BAAS	
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.

4. Roles and Responsibilities

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

Service Activities – Core Elements	Calligo	Customer
CO-CC-BAAS		
VM Level Backups Specification	C	A, R
Application-Level Backups Specification	C	A, R
VM Level Backups Configuration	A, R	C
Application-Level Backups Configuration	A, R	C
Backup Checks	A, R	I
Restore Testing	A, R	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

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

5. Reporting

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

Service Item	Reporting Item	Description	Frequency
CO-CC-BAAS	**Daily backup status report**	Report of all backup jobs ran on the last 24 hours	Daily

6. Data Residency

Calligo Data Residency

7. Service Requirements

Service Item	Requirements Item
CO-CC-BAAS	CommVault Proxy Server (only required for application-level backups)
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
Service Account with access to the client's file system. (This is a requirement for file level recovery.)

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

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 BaaS service, Calligo can provide the following service items as optional add on services for BaaS:

Service Item	Service Item Reference	Description
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 BaaS 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 BaaS 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.