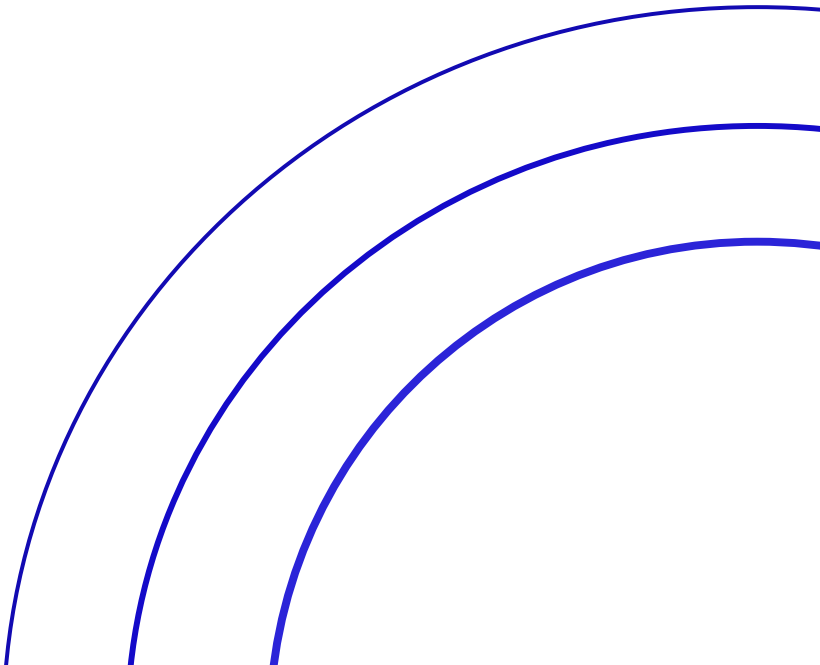
Security Awareness & Phishing Training Service Description



TITLE:	**Security Awareness & Phishing Training Service Description**	**DOCUMENT REF NO:**	QMS REC 205
DESCRIPTION:	This document defines the services provided by Calligo's Security Awareness & Phishing Training service		
OWNER/ AUTHORITY:	CISO	**VERSION NO:**	1.0
DOCUMENT CROSS REFERENCE:	None.	**VERSION DATE:**	19/03/2024
DISTRIBUTION METHOD	Email and Website	**DOCUMENT CLASSIFICATION**	Public

Contents

1. Service Overview

This document defines the services provided by Calligo's Security Awareness and Phishing Training. The Security Awareness and Phishing Training is one of a suite of services within the Calligo Operating Model.

2. Service Inclusions

2.1. SEC-MS-SAT

This service leverages Security Consultants and automated tooling to deliver security awareness and phishing training to a customer's end users on a defined schedule.

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. SEC-MS-SAT

3.1.1. Inclusions

SEC-MS-SAT	
Scope Item	**Description**
Configuration	Selection of security awareness and phishing training content and configuration of campaigns in accordance with client requirements.
Delivery	Delivery of online training content and phishing simulations to customer's end users as per the predefined schedule.
Reporting	Delivery of Monthly Business Reports.

3.1.2. Exclusions

SEC-MS-SAT	
Exclusion Item	**Description**
Custom Content Development	Creation of bespoke training modules or phishing templates beyond those available in the training platform.

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 Security Awareness and Phishing Training elements:

Service Activities – Core Elements	Calligo	Customer
SEC-MS-SAT		
Configuration of security and phishing training campaigns	R, A	C, I
Delivery of security awareness training content	R, A	I
Delivery of phishing simulations	R, A	I
Generating security training and phishing reports	R, A	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

This table represents the standard reports included in as well as the deliverable frequency.

Reporting Item	Description	Frequency
Monthly Business Report	A monthly report that provides a user audit report detailing which courses have been completed and further business insight into the Training and Phishing campaigns and user behaviour.	1 per month

6. Data Residency

Calligo Data Residency

7. Service Requirements

Requirements Item	Description
Training Topics	Customer to review list of available training topics and advise as to which they wish to include in the training campaigns.
Phishing Content	Customer to review list of available Phishing content and advise as to which they wish to include in the Phishing campaigns.
Target Users	Customer to provide names, email addresses and user group details of all end users to be included in the training and Phishing campaigns.
Excluded Users	Customer to provide names, email addresses and user group details of any end users they wish to exclude from the training and Phishing campaigns.
Campaign Schedule	Customer to confirm preferred dates and times for training content and Phishing campaigns release to end users.
Reporting Recipients	Customer to provide email addresses for contacts to receive the Weekly User Compliance and Monthly Business reports.

8. Access Requirements

Requirements Item	Description
Training and Phishing Platforms Allowlisting	Allow training and Phishing platforms' sender email addresses to send to end users.

9. Support Locations

Calligo Support Locations

10. Service Catalogue Request Items

Catalogue Item	Fulfilment Time	Qualifying Criteria	Included Requests
Security Awareness Training and Phishing Campaign Content Updates	5 days	Active training and phishing campaigns	1 update per month at no additional charge. The 1 update can include multiple training course updates.
Monthly Business Report	1 day	Completion of full calendar month with live users.	12 – 1 per month

11. Standard SLO's

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

Any clients onboarding to Calligo will require the following document as an introduction to service:

Calligo – Welcome to Support for Clients

12. Auxiliary Services

12.1. Service Onboarding & Transition

To launch the Security Awareness and Phishing Training successfully, service design, onboarding and transition will be required to prepare and test both the environment and the managed services processes. Calligo will conduct a workshop 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. Test criteria are captured and signed off, to allow for the Security Awareness and Phishing Training to commence.

12.2. 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.

13. Document Control

DOCUMENT OWNER & APPROVAL
The CISO 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.
Approved by CISO, Calligo ("Entity") on 19 March 2024

CHANGE HISTORY RECORD				
VERSION	**DESCRIPTION OF CHANGE**	**AUTHOR**	**APPROVAL**	**DATE OF ISSUE**
1.0	First version	InfoSec Manager	CISO	19/03/2024