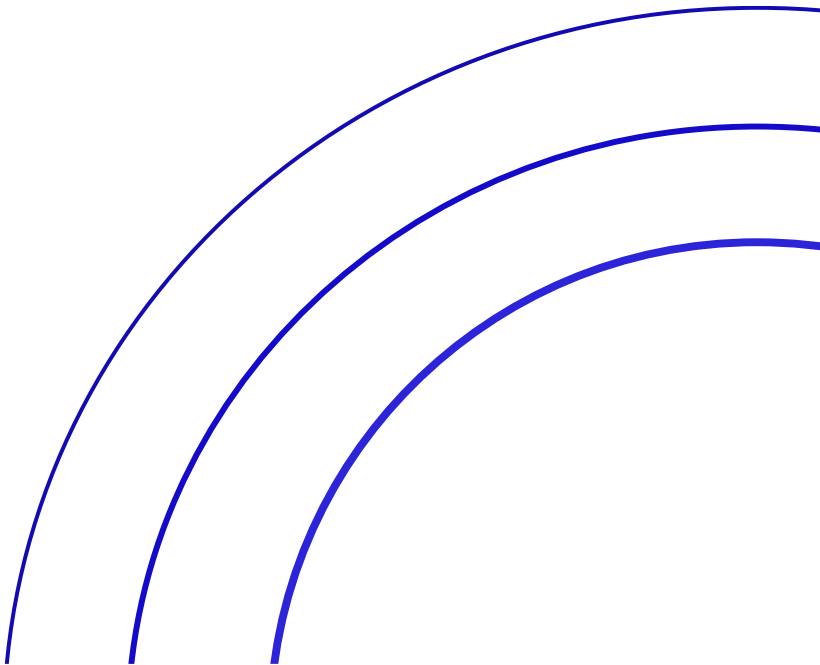
Network Penetration Testing
Service Description



TITLE:	**Network Penetration Testing Service Description**	**DOCUMENT REF NO:**	QMS REC 200
DESCRIPTION:	This document defines the services provided by Calligo's Network Penetration Testing service		
OWNER/ AUTHORITY:	CISO	**VERSION NO:**	1.0
DOCUMENT CROSS REFERENCE:	QMS REC 201 – External Network Penetration Testing Service Item QMS REC 202 – Internal Network Penetration Testing Service Item	**VERSION DATE:**	17/01/2024
DISTRIBUTION METHOD	Email and Website	**DOCUMENT CLASSIFICATION**	Public

Contents

1. Service Overview

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

2. Service Inclusions

2.1. CO-ITMS-PEN-E

This service provides external network penetration testing.

2.2. CO-ITMS-PEN-I

This service provides internal network penetration testing.

2.3. 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-ITMS-PEN-E

3.1.1. Inclusions

CO-ITMS-PEN-E	
Scope Item	**Description**
Configuration	Configuration of penetration testing and security assessment platform to execute penetration testing against customer provided target IP addresses and/or DNS names.
Testing	Execution of external penetration tests and vulnerability scanning against customer provided targets on agreed date and times.
Reporting	Delivery of Executive Summary and Technical Reports to the customer, along with supporting evidence. Reports to be presented to the customer by a Calligo Security Consultant.

3.1.2. Exclusions

CO-ITMS-PEN-E	
Exclusion Item	**Description**
Risk Remediation	Remediation of any identified risks requires Professional Services time.
Internal Testing	This element of the service requires **CO-ITMS-PEN-I**

3.2. CO-ITMS-PEN-I

3.2.1. Inclusions

CO-ITMS-PEN-I	
Scope Item	**Description**
Agent Deployment	Deployment and configuration of Ubuntu agent VM with access to the internal networks that are to be scanned.
Configuration	Configuration of penetration testing and security assessment platform to execute penetration testing against customer provided target IP addresses and/or DNS names.
Testing	Execution of internal penetration tests and vulnerability scanning against customer provided targets on agreed date and times.
Reporting	Delivery of Executive Summary and Technical Reports to the customer, along with supporting evidence. Reports to be presented to the customer by a Calligo Security Consultant.

3.2.2. Exclusions

CO-ITMS-PEN-I	
Exclusion Item	**Description**
Risk Remediation	Remediation of any identified risks requires Professional Services time.
External Testing	This element of the service requires **CO-ITMS-PEN-E**

3.3. CO-ITSM-SD

3.3.1. 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.

3.3.2. 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 Network Penetration Testing service elements:

Service Activities – Core Elements	Calligo	Customer
CO-ITMS-PEN-E		
Configuration of penetration testing platform	R, A	C, I
Execution of security assessments	R, A	I
Generating security assessment reports	R, A	I
Presentation of security assessment findings	R, A	C, I
CO-ITMS-PEN-I		
Deployment and configuration of agent virtual machine	R, A	C, I
Configuration of penetration testing platform	R, A	C, I
Execution of security assessments	R, A	I
Generating security assessment reports	R, A	I
Presentation of security assessment findings	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

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
Executive Summary Report	An executive summary report containing a high-level summary of the security vulnerabilities identified as well as a remediation roadmap.	1 per assessment
Technical Report	The technical report will consist of the specific details identified during testing. Throughout testing, the platform collects log information as well as captures screenshots to demonstrate proof of validation of identified vulnerabilities. The technical report also includes recommendations with regard to how to remediate the identified security vulnerabilities.	1 per assessment

6. Data Residency

Calligo Data Residency

7. Service Requirements

Requirements Item	Description
Consent	Consent required for Calligo to conduct internal security testing and vulnerability scanning across noted targets.
Agent host (Internal Scanning only)	Scanning agent runs on an Ubuntu Virtual Machine, which needs internal network access.
Target details	Customer to provide IP addresses and/or DNS names of target systems and services.
Exclusion details	Customer to advise of any exclusions if scanning a block of IP addresses.
Test date and times	Customer to confirm date and time window for conducting the assessment.
Notifications	Customer to provide email addresses for contacts requiring notifications for when each phase of the assessment kicks off and completes.

8. Access Requirements

Requirements Item	Description
Agent VM (Internal Scanning only)	Scanning agent runs on an Ubuntu Virtual Machine, which needs internal network access. Can be run from a spare workstation or VM host (VMware of Hyper-V) for on-premise networks. A temporary VM can be deployed for CloudCore environments.
Assessment Platform Allowlisting	Allow testing platform IP addresses to access target systems.

9. Support Locations

Calligo Support Locations

10. Service Catalogue Request Items

Catalogue Item	Fulfilment Time	Qualifying Criteria	Included Requests
Executive Summary Report	5 days	Successful completion of security assessment	1 per assessment

Catalogue Item	Fulfilment Time	Qualifying Criteria	Included Requests
Technical Report	5 days	Successful completion of security assessment	1 per assessment

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 Network Penetration Testing service 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 Network Penetration Testing service 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, Project Management Frameworks as well as the guidance and requirements of the CSSF.
Approved by the VP of Cloud Operations, Calligo ("Entity") on 17 January 2024

CHANGE HISTORY RECORD				
VERSION	**DESCRIPTION OF CHANGE**	**AUTHOR**	**APPROVAL**	**DATE OF ISSUE**
1.0	First version	CISO	VP of Cloud Operations	17/01/2024