Continuous Security Testing

Service Description

Version 4.1.2

claranet

Make modern happen®

Contents

Introduction

This Service Description describes the Service Claranet provides and details the Customer's responsibilities in relation to this Service. The Service Description forms part of the Agreement between the Parties and is subject to the terms of the Claranet Master Services Agreement set out at www.claranet.co.uk/legal or as otherwise agreed by the Parties and the Parties agree to be bound by such terms. Unless otherwise specified, all terms used within this document are in accordance with the terms to be found in the Master Services Agreement.

Claranet provides the following services as part of its Continuous Security Testing (often referred to as "CST" or the "Service"). The Service components of the Service are set out below along with the related material tasks and responsibilities for that Service component.

1. Scope of Service Description

The Customer expressly agrees that any services, activities and deliverables not expressly set out within this Service Description shall be out of scope for the Service. Any components which are described as optional or additional in this Service Description will be chargeable at additional costs, and will need to be purchased by the Customer and expressly referenced as such in the relevant Customer Order Form or Statement of Works.

The Customer may request a change to the Statement of Works required under this Service Description, but this will be chargeable at additional costs and to be agreed by the Parties signing an Order Form or Change Request. Claranet reserves the right to charge on a time and materials basis for any additional work.

Notwithstanding the foregoing, in the event Claranet completes additional services, activities and/or deliverables upon the request or at the direction of the Customer, Customer shall be responsible for the payment of all Fees and expenses associated therewith, whether or not an Order Form or Change Request has been executed in relation to the additional services or activities.

2. Service Overview

Continuous Security Testing (CST) helps you identify new vulnerabilities as they surface so you can patch them quickly to mitigate cyber risks to your organisation on an ongoing basis.

It's an approach that allows you to secure a whole range of applications with our help and advice. Once you have chosen the applications, Application Programming Interfaces (API) or external infrastructure you want us to test, we use a combination of manual penetration testing and vulnerability scanners to identify and verify vulnerabilities.

Your team gets access to the cyber portal where vulnerabilities are shared and prioritised according to their risk and impact. CST reduces the time to detect vulnerabilities in your application estate, and allows you to remediate them sooner. More importantly, it helps you reduce the workload for remediating vulnerabilities by doing it little and often.

With CST, your vulnerability management programme becomes fast and fine-tuned to your estate, with expert penetration testers on hand who become an extension of your security team.

3. Service

3.1. Service Tiers

Service Tiers are allocated to each Asset to determine the type and duration of testing to be conducted. Tiers are allocated based on the depth of testing as per your preferences, defined either by the criticality of the asset, or to accommodate budgets.

Tier	Description
0	Testing is limited to default automated unauthenticated scanning and manual vulnerability verification. Infrastructure testing will always be a Tier 0.
1	Testing is limited to default automated scanning and manual vulnerability verification. This tier also provides tailored options to include: Custom headers; Custom scanning intensity; Custom scanning profile; Custom Scanning time window; Authenticated Scanning.
2	As the above service with limited dedicated penetration testing per month, to discover advanced vulnerabilities.
3	As the above service with dedicated penetration testing time added to discover advanced vulnerabilities, recommended for complex applications.
4	As the above service with additional dedicated penetration testing time added to discover advanced vulnerabilities, recommended for complex and business critical applications.

3.2. Features for all Service Tiers

The following features are supported on all Service Tiers:

Feature	Description
Automated continuous scanning	Scanning of internet facing applications, external infrastructure and APIs, hereinafter, referred to as 'Assets'.
Manual verification of scanning results	• Removal of false positives and assessment of risks to ensure they are graded appropriately. • Evaluation of each vulnerability based on potential business impact. • Evaluation of each vulnerability based on the probability of exploitation, gauging difficulty and desirability of exploitation. • Classification of the vulnerabilities using the CVSS.
Open port monitoring	We scan your in-scope infrastructure to identify open ports and active services. Any variations from the previous month's scan are highlighted in the monthly report and potential issues are investigated manually.
Remediation support	On-demand support to enable report assimilation and support remediation efforts.
Re-testing of vulnerabilities	Re-testing of vulnerabilities is available at any point to verify a vulnerability has been remediated effectively. If fixed, we will email a report confirming the re-test results, if the problem isn't fixed we inform you by email.
High Impact Vulnerability Notification	A notification will be sent when a high impact vulnerability is verified. The notification includes a detailed description of the vulnerability, remediation advice and technical analysis with evidence and steps to reproduce.
Security Advisory (notification)	Our testers will provide details of zero-day disclosures that may be relevant to your environment. A Security Advisory will be issued explaining the nature of the exposure, type of affected systems/technologies and remediation advice.

	The CST team will also test all Assets in scope for the zero day vulnerability and if found a Vulnerability notification will be sent.
Cyber Portal	**Dashboard** • Single pane of glass to access live vulnerability data reported by our service, making it easier to manage your vulnerabilities and remediation activities. • Identify the most frequently occurring vulnerabilities. • Identify the most vulnerable Assets for focused attention. **Inventory (Asset Management)** • Manage your Assets in one place. • Categorise Assets using tags for better organisation (e.g., by department or region). • Stay informed about asset-related alerts. **Vulnerabilities** • Access a comprehensive list of vulnerabilities. • Show verified vulnerabilities with their CVSS score, impact and probability helping you prioritise what to fix first, together with remediation advice provided by our testers. • Ability to filter vulnerabilities by region, department, teams or any grouping of your choice. • Saved filters for commonly used filter configurations. • Filter by High Impact vulnerabilities. • Filter by Asset Tags to pinpoint specific areas. • Dive into the details of each vulnerability with just a click. **Reports** • Easily access all your reports in one place. • Monthly reports tailored to your specific vulnerabilities. • Ability to generate your own custom reports

	• Stay informed with notifications for High Impact Vulnerabilities and security advisories. **User Management** • A designated System Admin manages user access. • System Admin can add additional users to the portal for collaboration, using Role Based Access Controls. **Help section** • Comprehensive guide for portal features, navigation, and use. **User Manual** • Detailed documentation covering all aspects of portal operation. • Provides in-depth instructions and guidelines for users. **Tutorial Mode** • A visual and interactive learning tool to enhance user understanding. • Offers a practical walkthrough of portal features.
Monthly Report	At the end of each month, we will produce a monthly report which summarises all the findings that were identified during the testing cycle. The report will provide the following: **Executive Level** • Executive summary for internal reporting. **Management Level** • Prioritised list of vulnerabilities using the CVSS v3.1. • Graphical summary of the vulnerabilities sorted by impact and probability. **Technical Level** • Assessment results section with detailed description of the vulnerabilities and technical analysis with evidence and steps to reproduce.

	• Remediation advice with instructions and suggestions to be used by the Customers' remediation team. • A table with all high and medium impact vulnerabilities for prioritised remediation of urgent tasks/issues. • Remediated results section which includes all the vulnerabilities that have been remediated from the previous test cycle.

3.3. Features for Service Tiers 2 and above

The following features are supported on Service Tier 2 and above:

Feature	Description
Manual penetration testing	Security testing of internet facing applications to deeper coverage of the attack surface. Deeper analysis of vulnerabilities for more accurate risk assessment. Option to test pre-production and production environments.

3.4. Service Components

The Service is made up of the following components:

3.4.1. Scanners

This category includes scanners that are utilised by the testing team for the automated scanning elements of the CST Service.

3.4.2. CST Virtual Private Network (VPN)

The CST team connect to the CST Virtual Private Network (VPN) to ensure that any traffic pertinent to the CST service is easily attributed to the service by virtue of leaving the same public facing endpoint.

3.4.3. Cyber Portal

The Cyber Portal provides your teams visibility of Assets being tested and any related vulnerabilities and their fixed status. It is also the repository for the monthly report.

3.5. Service Billing

The CST setup fee and first monthly payment will be charged on the service start date agreed during project delivery.

4. Data Management

Data on the Cyber Portal is managed as follows:

4.1. Sovereignty

All data relating to the service is transitioned and stored in AWS, within the European Union.

4.2. Security

The following methods and tools are used to secure data:

4.2.1. Encryption

Claranet uses 256-bit AES-GCM symmetric encryption keys to protect vulnerability data, asset, username and password data. In accordance with Claranet's Internal Security policies, the testing team utilise full hard drive encryption and share data using public-key cryptography on a need-to-know basis. Encryption helps to protect integrity of data from unauthorised access, theft, or data breaches.

Transport Layer Security (TLS) is used to encrypt data in transit. TLS helps to protect data from eavesdropping, tampering, and other attacks. We use industry-standard TLS versions such as TLS 1.2 and TLS 1.3. And Secure File Transfer Protocol (SFTP) is used to transfer large files. SFTP is a secure protocol that provides encryption, integrity, and authentication for file transfers.

4.2.2. Access Control

Access controls limit the number of people who can access Customer data. Access controls include role-based access control, and two-factor authentication.

4.2.3. Internal testers

Claranet employees are required to treat all customer information as confidential and keep secure. Additionally, all employees receive a criminal records check, past employment references, and credit histories before they are given access to company data to ensure safe and secure handling of customer information.

Claranet maintains a high-level of security awareness by ensuring that all employees receive security and compliance training as part of their induction process and annually thereafter. In addition, Claranet conducts regular internal auditing of employee adherence to security policies and training needs.

Further details can be found within Claranet's Security and Compliance Overview, available upon request.

4.3. Backup and disaster recovery

We maintain data backups and disaster recovery plans to ensure that Customer data is not lost due to accidental deletion, natural disasters, or system failures.

4.4. Retention

Vulnerability data will be retained on the following basis:

- Unfixed vulnerabilities will be stored for the duration of the contract.
- Fixed vulnerabilities will be available for 12 months.
- All data related to your service will be deleted and non-retrievable 90 days after contract termination.
- When an employee leaves your company, it's your responsibility to remove them from the Cyber portal.

5. Testing Methodologies

In addition to Claranet's testing methodologies, CST uses the following:

- Open Worldwide Application Security Project (OWASP);
- Web Security Testing Guide (WSTG);
- National Institute of Standards and Technology (NIST) SP 800-115 Technical Guide to Information Security Testing and Assessment;

- Payment Card Industry Data Security Standard (PCI DSS) Information Supplement:

Note: The above are standard and widely adopted methodologies, further details are available upon request.

6. Reports and Notifications

Unless agreed otherwise in the Statement of Works, reports and vulnerability notifications will be uploaded to the cyber portal and an email notification will be sent to the designated contacts. Sample reports are available upon request.

7. Scoping and quotation

Claranet will work with you to establish the scope of the service you require and provide a quotation and proposal. You will be provided with a Scoping Form which gathers information about your IP address ranges and URLs and we will consult with you to select a Service Tier for each Asset (or group of Assets).

Once the Scoping Form is complete, the CST Solution Architect will determine the Application Type (see table below) for each Asset and may use passive Open Source Intelligence Gathering activities to help identify the publicly visible attack surface. The Service Tier, together with the Application Type will define the depth of testing for each asset.

Once the contract is confirmed, a Statement of Works will be completed, capturing the important information about the scope of the engagement, requirements and deliverables.

App Type	Description
Inf	Infrastructure is defined as the network devices or IP address ranges that are to be included in the scope. Infrastructure targets can be internal or external.
App-0	An App-0 is defined as a basic web application. Typical features of an App-0 would be a “brochureware site” with limited or no capability for interaction with any of the content. Sites built on common Content Management Systems platforms e.g. WordPress, Squarespace, Wix or Weebly may fit into App-0 if they have limited customisations applied to them.

App-1	App-1 is defined as an application that has some level of dynamic content, often referred to as the ability to Create, Read, Update, or Delete (CRUD) content from a system by interacting with web forms. App-1s will navigate using traditional linked pages where a user can navigate simply from one form to another. Applications that permit user login also require a more considered approach when testing post-authentication components, for example, when the user can make persistent changes seen by other users or administrators. Example applications for this level are sites with complex or multi-part forms (such as insurance application forms), ecommerce sites, or applications with complex authentication.
App-2	App-2 is defined as an application that is very large or exhibits characteristics of a 'single page application'. Large applications will have many interactive functions and multi-stage web-forms as well as connections to multiple databases. They will provide a user with a highly customised experience.

Responsibility	Claranet	Customer
Scoping Form: Completion of the scoping form, outlining all Assets that require testing. This will include all IP addresses and URLs of known systems. This will form the basis of the Statement of Works.		✓
Provide a primary and secondary contact for the setup and duration of the Service: To ensure the smooth delivery of the Service, the Customer must provide Claranet with a primary and secondary contact, with the necessary knowledge and experience to provide all necessary assistance to Claranet pursuant to this Service. The primary and secondary contact will be authorised to request scope changes for duration of the contract.		✓
Access to key staff and stakeholders: Ensure that staff and stakeholders (both internal and external where relevant) are available for meetings and/or workshops.		✓

Application Type: Categorisation of Assets by the level of functionality and interactivity provided by each system, to identify effort level and resources.	✓	
Tier level: Selection of the desirable service tier for each asset based on the testing requirements.		✓
Statement of Works (SOW): Captures the required work and enumeration of the in-scope Assets as well as in-depth description of the testing environment, methodologies and deliverables and capturing the Service Tier and Application Type for each Asset. The SOW will form part of the contract and will be updated upon any change requests during the contract period.	✓	
Authenticated testing[1]: Provision of credentials where these are needed or desired. Credentials will be required for the identification of missing patches or out of date software and/or the thorough penetration testing of interactive web applications.		✓

[1] Authenticated test of web applications provides the most thorough assessment of your systems however, we do not recommend performing potentially disruptive authenticated automated scanning of production environments. We will not perform authenticated scanning on production environments unless expressly requested to do so.

8. Ordering

By ordering Continuous Security Testing, you permit Claranet access to and permission to test “In Scope” Assets, enabling the Service to be performed in accordance with this Service Description.

Responsibility	Claranet	You
Provision of scope details: Inform and provide the appropriate details as to the nature of the security testing on the Information System, to individuals within your company, to users, third party information stakeholders, third party information service providers or any other parties likely to be affected by the security testing.		✓
Permits, consent and permissions: You permit, and have all appropriate consents, permits and permissions from your employees, agents and sub-contractors, that allow Claranet to conduct Continuous Security Testing.		✓
Personal data consent: Confirm that all consents, required from data subjects to enable personal data (as defined in applicable local legislation) to be disclosed to Claranet to the extent required to carry out the security testing, have been obtained.		✓
Authorisation for access to target systems: Confirm that, in accordance with the Computer Misuse Act or any other applicable legislation (as amended) based on the locality of the assets and jurisdiction of the Agreement, all necessary authorisations and permissions to test, perform Services and that access to target systems will be provided to Claranet for the purposes of security testing, including, where necessary, modifications that demonstrate the impact of the exploitation of a vulnerability.		✓
Data protection: Take all measures to protect the Information System from any loss or damage that may arise because of the security testing.		✓
Data backup: Prior to commencement of, and regularly throughout, the security testing, you will take copies of information, data and applications or use any other methods available to you, to ensure the safety and protection of material within the Information System as you see fit.		✓

9. Onboarding

Once the Statement of Works is accepted, Claranet will build your service and commence testing activities. During this phase you will collaborate with the CST Team discussing the context of each target, gathering the essential information e.g., what the target is, known system fragilities, contact details (system owners, distribution groups for alerts), permitted scan times and any associated compliance requirements will allow us to manage your service. Your cyber portal access will also be setup.

9.1. Whitelisting

It's necessary for you to whitelist our IP ranges prior to onboarding. The penetration testing activities will test for thousands of vulnerabilities across your Assets. Any Intrusion Prevention System or Web Application Firewall that you have installed is likely to detect many of the signatures and therefore block several penetration testing activities. If your Intrusion Prevention System prevents further connections, the test will become ineffective at identifying vulnerabilities that could otherwise be exploited. To counteract this, the CST team will confirm the IP addresses used for testing so that these can be whitelisted, thereby allowing the testing to continue throughout the system. There are two key reasons we ask for this:

Attackers only need to find one exploitable vulnerability
Claranet's role is to find all vulnerabilities. Attackers can be very specific in the flaw that they are looking for. Malicious attacks do not always begin with a general scan to find all known vulnerabilities but can focus on a subset of high impact flaws. This approach has a much lower chance of being detected by your Intrusion Prevention System and is difficult to emulate without creating many false negatives and taking more time.

Attackers ignore privacy laws
To circumvent your Intrusion Prevention System an attacker will often change their IP address using TOR (https://www.torproject.org/). Whilst this is a powerful hacker tool it cannot be used in scanning because of privacy concerns; - penetration testing activities could exit the TOR network via an attacker-controlled host where sensitive vulnerability data could be captured.

Responsibility	Claranet	You
Whitelisting - Provision of IP addresses: To provide the IP addresses that are used for the penetration testing and scanning.	✓	

Whitelisting - Adding the IP addresses to the whitelist: Ensure that all default protections e.g., Web Application Firewalls and Intrusion Protection Systems have whitelisted the IP addresses provided by Claranet.		✓
Notification to third parties: Ensure all third parties e.g., hosting providers, cloud service providers, are notified that the testing is taking place.		✓
Vulnerability Notification: By default, Vulnerability Notifications will be issued for “High Impact” findings. This can be tailored to accommodate your preferences.	✓	
Contacts will be captured and maintained in the Statement of Works and confirmed during the onboarding call. This also applies to capturing Portal contacts to access Vulnerabilities, Reports and Alerts, and methods which can be phone and/or email.	✓	
Resolving a vulnerability: Fixing a reported vulnerability is required to ensure it will no longer appear in the reports. Failure to fix a vulnerability means that it will continue to be reported on and checked by Claranet, thereby reducing the available time and undermining the ability of the Continuous Security Testing team to identify new vulnerabilities.		✓

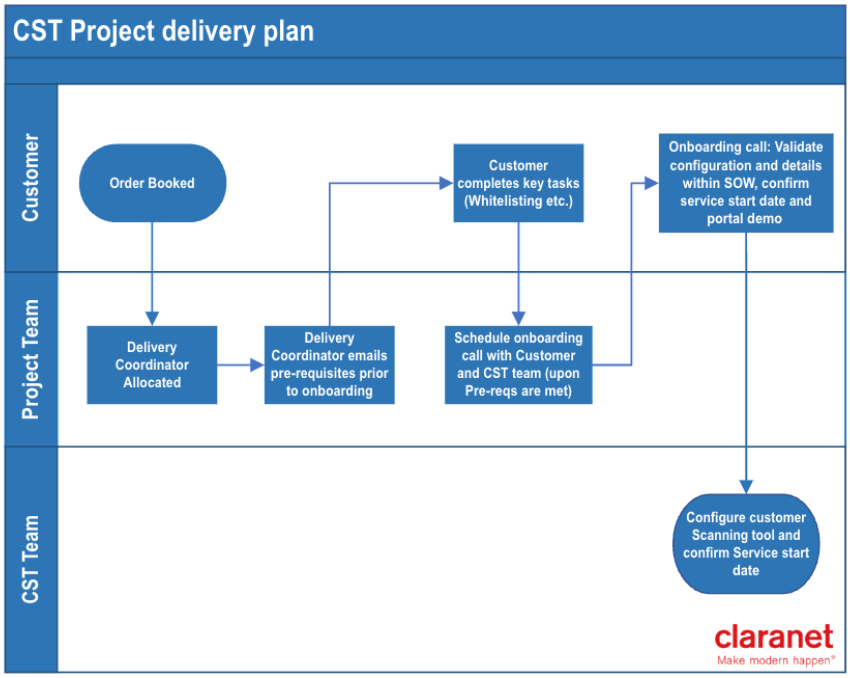
10. Project Delivery

10.1. Delivery coordinator

A Delivery Coordinator will be allocated to coordinate the onboarding of the Service.

10.2. Delivery plan

Typically CST will take 1 week to onboard from the receipt of the order.



11. Change Management

Claranet shall request written approval from you before a change can proceed to be implemented and if any specific time for implementation is required. Below is a list of Change types:

Change type	Definition	Example Changes
Simple Change Request (SC)	A simple change is one that carries a low impact on the Service or business operation.	• Pause testing of an asset. • Change or removal of key contact(s). • Monthly report customised according to your needs. • Vulnerability status change i.e., unfixed vulnerability to be changed to acceptable risk within the monthly report. • Change to the scanning window e.g., scanning is scheduled weekdays 0900-1700, or not at the weekend.

		• Configuration change such as IP address, website name, whitelisting. • By default, the scanner will be configured with 10 threads, these can be reduced if required.
Complex Change Request (CC)	A complex change is one that carries a moderate to high impact to the service or business operation. Where Claranet deems a change to be complex (warranting specialist engineering or excessive time and resources to plan and execute), then Claranet may advise on a charge for these requests. Claranet will assist in making clear as to whether or not a given request is determined to be chargeable.	• N/A
Complex-Contract-Affecting Change Request (CCA)	A complex-contract-affecting (CCA) change is where the request alters the Service in such a way as to no longer operate in the manner set out under the original Statement of Works. CCA's may have an impact on the ongoing billing or commercial agreement of the Service. Claranet will assist in making clear as to whether or not a given request is determined to be complex-contract-affecting. Once a change request is implemented the SOW will be updated and authorised by both parties before being implemented.	• New asset added to scope. • Change of asset. • Permanent removal of an asset from scope.

12. Service

This section provides an overview of the Service following implementation:

12.1. Hours of Service

Service	Hours of Operation
Automated Scanning	Scanning windows will be captured in the Statement of Works
Manual Penetration Testing	Monday to Friday 0430 - 1730 GMT excluding UK public holidays
Customer Support	Monday to Friday 0430 - 1730 GMT excluding UK public holidays

12.2. Service KPIs and metrics

Issue type	Target response time	Delivery method
High Impact Vulnerability Notification	15 minutes from verifying the vulnerability	Emailed to the designated contacts and published in the cyber portal.
Security Advisory Notification	24 hours from identification	As above
Monthly reports	Monthly	As above

12.3. Service Level Agreement and Service Credits

SLA calculations assume a requirement of continuous uptime of the Service, 24/7 all year round, which will be measured monthly based on the table below:

Service Availability Table:

Service	Monthly availability	Service Credit
CST	99.5%	5% of the Monthly Fee
CST	Less than 99.5% but more than 95%	8% of the Monthly Fee
CST	Less than 95%	10% of the Monthly Fee

Note: A breach of an SLA is not in itself a breach of the Agreement.

12.4. Service Priority Levels and Service Credits

Category	P1	P2	P3
Definition	All Service Components are unavailable, impacting the performance of the Service.	More than one component of the Service has failed, impacting the performance and availability of the Service.	One component of the Service has failed.
Acknowledgement	Within 4 business hours from the point of classification.	Within 8 business hours from the point of classification.	Within 8 business hours from the point of classification.
Notification Process	Email cst-management@claranet.com	Email cst-management@claranet.com	Email cst-management@claranet.com
Acknowledgement SLA Service Credit	5% of the Monthly Fee	5% of the Monthly Fee	N/A

12.5. Claiming Service Credits

In the event that Claranet has verified that it did not meet its response time as per Service Priority 1 or 2, or the Service Level Agreement uptime, Claranet will raise a credit note to the Customer's account that they can use to offset their standard monthly bill. Service Credits will be based on the applicable percentage of the monthly Fee, as detailed in sections 13.3 and 13.4 and will be calculated from the Service uptime. The maximum amount of Service Credit a Customer can receive in each calendar month relating to this agreement is limited to 50% of the Monthly Fee for the affected Service. Such Service Credits are pre-agreed liquidated damages and, unless stated otherwise in the Agreement, such Service Credits will constitute your sole and exclusive remedy with respect to the breach of SLAs.

Responsibility	Claranet	You
Reporting a Breach of an SLA: Claranet does not proactively report for SLA's, thus, you must report an SLA breach to claim for Service Credits.		✓
Verifying and Measuring SLA: Claranet will verify the SLA breach by confirming Service uptime. The Service downtime will be measured from the point the breach is reported (subject to being verified) up until it is resolved.	✓	

Note: The Customer's right to any Service Credit is not automatic. The Customer must submit a claim for Service Credits, in writing (by email), within 30 days from the validation of the Service Level Agreement breach to which they refer. All claims must be submitted to the appointed Account Manager and/or Service Manager. Requests for support received by Customer Support by means other than email (for example, telephone, fax) will be excluded when calculating any alleged breach of the Service Level Agreements.

Exceptions

Claranet excludes responsibility for meeting any Service levels to the extent that meeting the Service levels is affected by the following exceptions hereunder and Service Credits will therefore not be paid if the outage occurs from such exceptions:

- Where the Service has not been accepted by the Customer or has not been delivered by Claranet;
- Where Claranet has not met a Service Level Agreement due to Customer's failure to minimise the recurrence of problems;
- Where Claranet has not received an email from the Customer reporting an SLA breach; and
- Where the Service is disrupted or not available due to:
    - the Customer's failure to adhere to Claranet's reasonable instructions, and implementation, support processes and procedures; or
    - changes initiated by the Customer whether implemented by the Customer or by Claranet on its behalf.;
- Where the Customer is in default under the Agreement;

- In the event that the Service is unavailable due to the Customer being subject to cyberattacks;
- Where the Service is unavailable due to any failures that cannot be corrected because you are inaccessible or because Claranet personnel are unable to access your relevant systems;
- Where any non-availability is caused by any periods of schedule maintenance or emergency maintenance initiated by either Parties;
- Where the Service is unavailable due to changes initiated by the Customer whether implemented by the Customer or by Claranet on its behalf;
- Where the Service is unavailable due to viruses;
- Where the Service is unavailable due to the Customer's failure to adhere to Claranet's implementation, support processes and procedures;
- Where the Service is unavailable due to the acts or omissions of the Customer and its employees, agents, contractors or otherwise;
- Where third party contractors or vendors or anyone gaining access to Claranet's network, control panel or to the Customer's website at its request;
- Where the Service is unavailable due to a force majeure event;
- Where the Service is unavailable due to any violations of Claranet's Acceptable Use Policy;
- Where the Service is unavailable due to any event or situation not wholly within the control of Claranet;
- Where the Service is unavailable due to the Customer's negligence or wilful misconduct or of others authorised by the Customer to use the Services provided by Claranet;
- Where the Service is unavailable due to any failure of any component for which Claranet is not responsible, including but not limited to electrical power sources, networking equipment, computer hardware, computer software or website content provided or managed by the Customer;
- Where the Service is unavailable due to any failure of local access facilities provided by the Customer; and
- Where the Service is unavailable due to any failures that cannot be corrected because the Customer is inaccessible or because Claranet personnel are unable to access the Customer's relevant sites.

12.6. Points of contact

Purpose	Who to contact	Contact Info
Change Requests	CST Support	uk-cst@claranet.com, Cyber Portal
Vulnerability remediation support and request a re-test	CST Support	uk-cst@claranet.com
Customer Support	CST Support	uk-cst@claranet.com
Escalations and complaints	CST Manager	cst-management@claranet.com

13. Assumptions

If the assumptions listed below are not met, the Service delivery may be affected and any Service Levels set out herein are impacted, Service Credits will not apply as a result:

- The Customer will provide the necessary support and relevant personnel to ensure the success of the project;
- All work will be carried out remotely with no requirement to visit the Customer's site(s) unless agreed otherwise;
- Claranet will have appropriate access to all systems to successfully complete the project;
- Effective whitelisting and access to credentials are required to perform authenticated scanning and testing;
- Any changes to the scope could result in a revision to the testing timelines and costs;
- This project will not have an impact on any other existing projects;
- The information provided by the Customer is complete, accurate and up-to-date;
- The Customer will provide reasonable and timely cooperation and follow instructions as required by Claranet;
- The Customer will inform Claranet of any scheduled maintenance or emergency maintenance within reasonable notice that will affect the Service's performance in scanning, verifying, and identifying vulnerabilities within your Assets; and
- The Customer will ensure that technical details are kept up to date by submitting a Change Form to Claranet to confirm or update their relevant details.

14. Boundaries of the service

Conducting the Continuous Security service involves the testing of your live systems on your current infrastructure. This may therefore have an impact on current workloads and environments, and these will be discussed with you prior to commencement and minimised wherever possible. To this end, you will appoint at least one employee who shall act as liaison between yourselves and Claranet. They must have substantial experience of your computer systems, networking and project management of your information systems.

Responsibility	Claranet	You
Operational involvement: No intentional interference will be caused to the operation of your information system, unless it is with your express authority.	✓	
Boundary violations: Inform you of any violations of any test boundaries that occur. In the event of any boundary violation, Claranet will cease testing, document the extent of the violation and inform you as soon as is practicable.	✓	
Minimising Issues: You agree to correct problems and to attempt to minimise the recurrence of problems, for which you are responsible, that may prevent Claranet from meeting the SLAs.		✓
Liaison: Provide an employee as liaison with Claranet that is technically familiar with your systems as described.		✓

15. Terminology

Unless otherwise specified, capitalised terms used in this Service Description shall bear the same meanings as those used in the Master Service Agreement unless otherwise expressly stated herein. Set out below are a description of key technical terms used in this Service Description.

Terms	Definition

Application Programming Interface	Refers to a way for two or more computer programmes to communicate with each other.
Assets	Refers to the Customer's internet facing applications, External Infrastructure and APIs
Common Vulnerability Scoring System	Refers to the free and open industry standard for assessing the severity of computer system security vulnerabilities.
National Institute of Standards and Technology (NIST) SP 800-115 Technical Guide to Information Security Testing and Assessment	Refers to a cyber framework that helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data.
Open Worldwide Application Security Project (OWASP)	Refers to an online community that produces freely available articles, methodologies, documentation, tools, and technologies in the field of web application security.
Payment Card Industry Data Security Standard (PCI DSS) Information Supplement	Refers to an information security standard used to handle credit cards from major card brands.
Web Security Testing Guide (WSTG)	Refers to a comprehensive Open Source guide to testing the security of web applications and web services.