Claranet UK

Security Risk Assessment

Service Description v2.5

claranet® | helping our customers do amazing things

Contents

1. 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 Security Risk Assessment ("Service"). The Service components of the Service are set out below along with the related material tasks and responsibilities for that Service component.

2. 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 Work.

The Customer may request a change to the scope of work 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.

3. Service Overview

Claranet's Security Risk Assessment Service is key to risk management and drives the Customer's risk strategy.

Customers can use the Service to understand threats, identify risk across their organisation, establish a baseline security performance, track changes and improvements over time, and take pragmatic action to mitigate risk to an acceptable level.

Claranet's Service is tailored to each Customer and will enable Customers to evaluate, analyse and improve their security posture, on an ongoing basis, according to their needs. The outputs of assessment include: a detailed risk index, validation of the effectiveness of security controls and processes, and guidance on the controls needed to address security risks including the implementation of such controls.

4. Service Components

4.1. Comprehensive 360° Risk Assessment

Claranet's assessments focus on what need to be protected, how the Customer is currently protecting their business and where there are risks within the Customer's environment.

Aligned with external frameworks (e.g. ISO 27005, NIST)

- A defence in depth assessment, threat modelling, and vulnerability assessment to ensure an organisation's security The purpose of the threat modelling is to identify sources of threat information relevant to the organisation.
- Holistic view and may identify multiple threats.
- This assessment looks to characterise threat sources of concern, how capable they are and their intentions for targeting a business. In simple form it quantifies the probability of identified threats becoming a real risk.
- Uses both qualitative and quantitative security risk assessment methods.
- The qualitative method visually represents the relative severity of the various risks the business faces, whilst the quantitative assessment enables a business to make cost effective decisions and manage the risks for the entire asset lifecycle.

4.2. Information Security Risk Assessment

Aligned with ISO 27001

- Looks at a wide and thorough overview of the Customer's security systems and operations, involving identifying and assessing risks to the confidentiality, integrity and availability of the Customer's assets.
- Evaluates the Customer's current information security environment, scrutinising applications, systems, people and processes.
- It provides in-depth reviews of the systems physical attributes, identifies gaps in the security policies/ controls and conducts vulnerability evaluations.
- Validates conformance with security policies.
- As a business the Customer should not expect to eliminate all risks; rather, must seek to identify and achieve an acceptable risk level for the organisation. The goal is to treat risks in accordance with Customer's overall risk tolerance.

4.3. Condensed Information Security Risk Assessment

Aligned with the IASME Cyber Assurance

- A condensed information security management standard framework, designed as a more cost-effective approach to support organisations to achieve an excellent level of information security.
- Maps to the Governments 10 steps to Cyber Security, NIS Directive and ISO27001.
- This assessment provides a review against the following control themes: incident response and business continuity; IT backups; data protection; policies; operational management; training; and managing people, physical and environmental cyber security and technical intrusion.
- Focuses on implementation of new ways to secure organisational data and services, improving existing ones and to increase the level of security knowledge within the business.

4.4. Roles and Responsibilities

The Customer shall cooperate with Claranet and be responsible for the performance of its resources, representatives and agents in the Customer's Roles and Responsibilities in this Service Description.

The Customer acknowledges and agrees that Claranet's performance of the Service is dependent upon, among other things, by the timely access to all data, information and personnel by Claranet, that all information provided is accurate and up to date as well as the timely and effective completion of the Customer's Roles and Responsibilities as set out herein or requested of the Customer from time to time by Claranet.

Responsibility	Claranet	The Customer
Engagement start: Claranet consultant will commence the Service on the agreed date, either onsite or remotely via Microsoft Teams, or another suitable mechanism if Microsoft Teams is not suitable	✓	
Provide a suitable primary contact for the length of the Service: To ensure the successful completion of the engagement, the Customer must provide Claranet with a primary contact with the necessary knowledge and experience to provide all necessary assistance to Claranet pursuant to this Service Description and/or SOW.		✓
Plan: Upon commencement of the consultancy, the Claranet consultant, together with the Customer's primary contact, will formulate a plan for the engagement to allow the primary contact to arrange any necessary site visits and/or meetings with stakeholders required to successfully complete the engagement.	✓	✓

Responsibility	Claranet	The Customer
Supply documentation/information: Ensure that the Claranet consultant is promptly provided with all information that is requested and needed to perform the Service effectively.		✓
Arrange site visits: Ensure that the Claranet consultant has access to all sites required to complete the engagement.		✓
Access to key staff and stakeholders: Ensure that key Customer's staff and stakeholders (both internal and external where relevant) are available for meetings and/or workshops.		✓
Provide a suitable working environment: Where Claranet employees are required to attend customer and/or third party premises, it is the responsibility of the Customer to ensure Claranet employees are provided with a suitable, safe working environment.		✓
Sharing the documented methodology: Claranet will share the latest methodology.	✓	

5. Reporting

Once the consultancy is complete, a bespoke report is produced which will typically include:

- Executive summary
- Graphical summary (dependent upon specific objectives)
- Risk Register
- Consultancy findings.

Executive summary

This provides a high-level summary of the key findings from the consultancy. This section includes any constraints and restrictions encountered during the consultancy and next steps.

Graphical summary

Graphical representation may be provided within the report, which will be dependent upon specific objectives.

Consultancy findings

The bulk of the report concentrates on providing details of the findings from the consultancy. The specific findings documented within the body of the report will be dependent upon the specific business objectives agreed within the SoW.

5.1. Quality Assurance

At the completion of a report, it is passed through a Quality Assurance (QA) process within Claranet where it is reviewed by senior colleagues. Any amendments or changes that are suggested are then fed back to the Claranet security consultant(s) that are involved in the delivery of the Service so that these can be applied.

It is then sent directly to the Customer's primary contact(s) by the pre-agreed and appropriately secure method.

Full final reports are completed typically within 10 Working Days, although this may take longer in the cases of larger projects or where there are delays in Claranet receiving the information. Where results are required by a specific date, this needs to be agreed during the scoping.

5.2. Timescales

The length of time spent producing the report is determined at the scoping and prepare for testing stage and will be included within the consultancy time.

Where a final report is needed by a specific date, Customer must inform Claranet as early as possible so this can be accommodated. Claranet will endeavour to accommodate the request and will discuss these with the Customer at the scoping and prepare for testing stage. This is to ensure that adequate resource can be assigned to the production and QA of the Customer's reports for the specified time.

6. Delivery Matters

6.1. Service Deliverables

Once the Service engagement is complete, Claranet will produce a report and securely share this with the Customer.

The Customer agrees that all Intellectual Property Rights in any Service Deliverables shall remain the property of Claranet, and that Claranet, upon receipt of payment in full, hereby grants to the Customer a non-exclusive, non-transferable licence to copy and use the contents of such Service Deliverables for its own internal purposes only.

6.2. Fees and Payment

Fees payable under this Contract will be invoiced on delivery of the Services. If no report is to be provided, fees are payable on completion of the final engagement day.

Pre-ordered days which are not paid for up-front and are not used within 12 months of the date of the related Order Form, then Claranet will invoice the unused days 3 months prior to the end of such 12 month period and the Customer will then have 3 months to schedule or utilise the remaining pre-ordered days.

6.3. Delays and cancellations

Following the agreement of the Service Commencement Date, Claranet will allocate resources and facilities and will therefore commit to any third party expenditure to fulfil its contractual commitments. Should the Customer wish to re-schedule or cancel the Service after this point, this will be subject to Claranet's absolute discretion. The Customer agrees that it may have to pay Claranet a cancellation or reschedule fee as set out below as losses which Claranet will incur due to the cancellation or re-scheduling.

Cancellation timescale	Cancellation fee (% of engagement price)
Cancellation request received more than 30 working days prior to start date.	25% payable
Cancellation request received 8 to 30 working days prior to start date.	50% payable
Cancellation request received within 7 working days of start date.	90% payable

Reschedule timescale	Reschedule fee (% of engagement price)
Re-schedule request received more than 30 working days prior to start date.	0% payable
Re-schedule request received 8 to 30 working days prior to start date.	25% payable
Re-schedule request received within 7 working days of the start date with a firm re-booking date.	50% payable

Unavoidable absence

Should a Claranet consultant allocated to the delivery of the Service become unavailable at short notice for reasons that are commercially unavoidable (for example, sickness) then every attempt will be made to provide a replacement at the earliest possible opportunity. In these circumstances, whilst some delay is usually inevitable, Claranet will endeavour to minimise the impact on the delivery of the Service.

Expenses and travelling

Expenses are charged at cost for travel, accommodation, and sustenance where onsite work is required. Claranet can provide the Customer with an estimate of any likely expenses during the sales order process. To ensure accuracy and the lowest costs possible, expenses are charged upon completion of the consultancy unless otherwise agreed.

For onsite work, Claranet will plan the schedule of the engagement, taking into account travel time. Customers are not normally charged for time incurred during travelling, but will be expected to pay for travel costs. Where travel delays are incurred the Claranet consultant will inform the Customer to provide an estimated time of arrival and, where possible, will make up any time lost by travel delays during the engagement.

7. Assumptions and Exceptions

Service delivery may be affected if the following occur below. Where relevant and to the extent any Service Levels set out herein are impacted by the below, Service Credits will not apply as a result.

(a) It is assumed that where required as part of the Service, access to the Customer's IT infrastructure or testing environment is quickly established and retained for the duration of the Service. Any issues relating to access and permissions may result in work being halted or delayed until such access is resolved, or cause failures in delivery because Claranet personnel are unable to access the Customer's relevant sites.

(b) Where software licences are not provided as part of the Service, it is the Customer's responsibility to ensure they have the appropriate subscriptions and licences as required to benefit from the Service. The costs of such licences and subscriptions are not included in the price of the Service as set out in this Service Description unless otherwise provided in the Agreement.

(c) Claranet is not responsible for any failure of any component for which Claranet has no control over, including but not limited to electrical power sources, networking equipment, computer hardware, computer software or website content provided or managed by the Customer.

(d) Where the Service is disrupted or not available due to:

1. the Customer's failure to adhere to Claranet's implementation, support processes and procedures
2. changes initiated by the Customer whether implemented by the Customer or by Claranet on its behalf
3. the Customer exceeding system capacity
4. the acts or omissions of the Customer and/or its employees, agents, contractors or otherwise, including anyone gaining access to Claranet's network, control panel or to the Customer's website at the Customer's request
5. any failure of local access facilities provided by the Customer
6. any periods of scheduled maintenance or emergency maintenance
7. a force majeure event, or any event or situation (such as viruses or otherwise) not wholly within the control of Claranet
8. unauthorised users or hackers, or due to any violations of Claranet's Acceptable Use Policy.