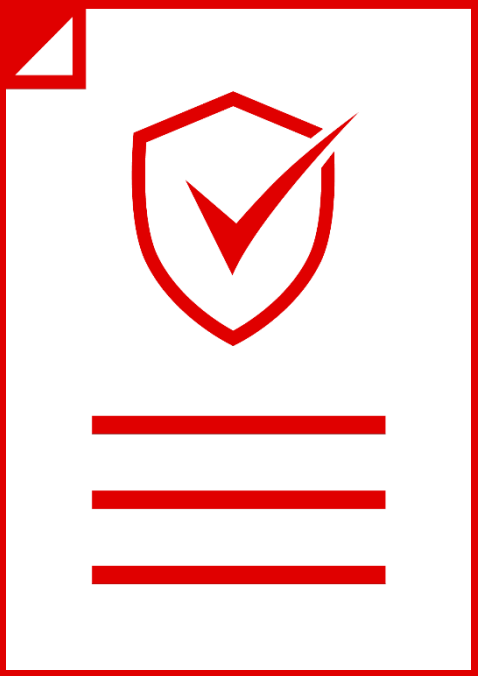

Claranet Cyber Security Service Description

PCI Consultancy Services

v.1.3

Sec-1 part of claranet cyber security

Contents

Service Overview

PCI Consultancy is delivered by, or led by, one of Claranet Cyber Security's QSAs (Qualified Security Assessor). This consultancy led engagement will utilise the Assurance team's wealth of knowledge to provide expert consultancy services to help organisations fulfil their PCI DSS (Payment Card Industry Data Security Standard) obligations.

Your engagement will be technically scoped by a member of the Assurance Team, carefully mapping out the size of the payment environment and the various payment channels in use.

The deliverable from PCI Consultancy is either a report to help the business with its PCI DSS journey and specific objectives, or the completion of Self-Assessment Questionnaires (SAQs), a Report on Compliance report (ROC) and/or Attestation of Compliance reports (AOCs). Alternatively, a deliverable may be in the form of specific advice via email or over the phone. Deliverables are defined within the service specific methodologies.

PCI Consultancy consists of a wide range of service offerings, including but not limited to, Cardholder Data Environment (CDE) Mapping exercises, GAP Analysis, Assisted SAQs, PCI Credits and On-site QSA ROC Assessments.

PCI Consultancy is a manual service, delivered either onsite or remotely between 09:00 to 17:30 hours, Monday to Friday. This document will take you through the diverse options available to you and the stages of the process including responsibilities and obligations for you, our client and Claranet.

Anything not included in this Service Description will not be provided by Claranet as part of the PCI Consultancy service unless otherwise agreed by the parties in any Statement of Work (SoW) and/or Order Form together with any additional charges that may be applicable.

This document describes the service Claranet Cyber Security provides and details your responsibilities in relation to this service. The Service Description forms part of an agreement between the parties and is subject to the terms of the Claranet Master Services Agreement set out at claranet.co.uk/legal or as agreed by the parties and the parties agree to be bound by such terms.

Scope

By working closely with you during the initial scoping phase, we ensure that the service is suited to your specific requirements. This initial phase is to assist in defining an appropriate scope for consultancy delivery.

Initial discussions

Information regarding the scope of the consultancy can be provided by completing the scoping document. Initial discussions may also take the form of a conference call, face to face meetings or a WebEx. During this stage, we will discuss the challenges and requirements you have and which of the many PCI services are best suited to your needs. For more complex and bespoke engagements, it may be necessary to arrange a workshop in support of the creation of a scoping document and subsequent Statement of Work which may consist of multiple PCI services or elements from different service offerings.

Scope of Work

The Scope of Work, or Scoping Document, will need to be completed by you prior to Claranet providing costings and a proposal document. It will allow for a defined Statement of Work to be produced along with a prescription of the number of days the consultancy will take to complete. Most PCI Consultancy will be defined by objectives of the consultancy. These will form the basis of the Scoping Document, which will:

- Identify the drivers and goals for the consultancy
- Specify the main location from where the start of the consultancy will take place
- Specify any additional geographical areas and number of site visits required (specific locations may be confirmed during the consultancy)
- Suggest the ideal timescales for your consultancy

Areas considered during scoping

Consultancy will be defined by site visits, types of payment channels in use, number of different payment channels in use, the duration of the engagement defined by how many days a security consultant will need to complete the assessment based on the appropriate Claranet Cyber Security Methodology. Areas commonly considered during the scoping will include:

- Number of physical site visits required

- Number of team meetings required
- Number of payment channels in use
- Number of SAQs needed to be completed
- Type of client (Merchant/Service Provider)
- Size of the CDE

Statement of Work

Once the Scoping Document has been completed, a member of the Assurance Team will examine the information provided and apply a rigorous and consistent approach to ensure that sufficient time is allocated to the engagement to meet the objectives; the result of this exercise is the Statement of Work. The notes added to the Statement of Work are based around how Claranet Cyber Security will complete the consultancy. e.g. a breakdown of activities/tasks to be completed during the consultancy.

Inaccuracies in information provided during the scoping process may result in Scope Creep. Where Scope Creep occurs, resulting in the full consultancy not being completed during the agreed timeframe, additional charges will be required to complete the consultancy. This will be communicated during the consultancy stage.

Recommendation

Claranet Cyber Security will make recommendations regarding what consultancy best fits your requirements and return a Statement of Work to you.

A quote, or proposal document where appropriate, will be provided defining the costs, including any expenses, of the exercise. A sales order form will be produced as a final document for signature.

Responsibility	Claranet	You
Proposal and Statement of Work: Provide a high-level quotation/proposal detailing the structure, price, and delivery duration for the engagement and in accordance with the details outlined in the Scoping Document, produce a final Statement of Work and a sales order form for signature.	✓	
Scoping Document: Provide accurate information required by Claranet relevant to the consultancy and in support of a comprehensive engagement. This information will form the basis of the consultancy, so it is your responsibility to ensure that the information is made available and is accurate.		✓

Responsibility	Claranet	You
Recommendations: Make recommendations as to which PCI Consultancy service best meets the organisations objectives.	✓	
Transparency: Claranet's aim is to maintain transparency in all services offered to clients. To meet this aim, Claranet will highlight any areas of concern which may introduce Scope Creep into the project, resulting in additional consultancy charges. i.e., additional payment channels being identified during the consultancy.	✓	

Prepare for consultancy

The design of your consultancy depends largely on the size and complexity of the payment environment being used.

Scheduling

Consultancy can be scheduled upon receipt by Claranet Cyber Security of a purchase order. Your account manager can provide an indication of the potential availability of suitable security consultants at any stage. We will work with you to get the consultancy underway as quickly as possible, however, resource availability changes rapidly and the allocation of security consultants will only be confirmed once a purchase order has been received.

Responsibility	Claranet	You
Identify a timescale: Provide potential timeframes through your account manager for delivery of the work. As the availability of resources changes rapidly, these timeframes are indicative only and cannot be confirmed until a purchase order has been received.	✓	
Scheduling dates: Agree the consultancy dates and ensure availability of all stakeholders, internal and third party, required during the consultancy and the accessibility of site locations.		✓
Documentation availability: Provide access to all supporting documentation required by the security consultant during the consultancy.		✓
Reserve and allocate resources: Once the purchase order has been received, the dates for your consultancy can be confirmed and security consultant(s) can be assigned.	✓	

Cancellation and delays

Claranet Cyber Security will allocate the appropriate number of security consultants to your service. In the event of a delay or cancellation before or during the consultancy, the appropriate fee will be payable. Details are in the **Appendix**.

Where access to key stakeholders, or access to required site locations are unavailable prior to the commencement of the consultancy, Claranet Cyber Security may decide, for the benefit of all parties, to delay

and reschedule the engagement. Where this is the case, an appropriate rescheduling fee will be applied (see **Appendix**).

Communication

Clear lines of communication are critical to an efficient engagement, covering the transfer of information, how this is achieved, the frequency and the personnel involved. Describing the key personnel on both sides who are responsible for the delivery of the consultancy, ensures that any issues can be acted upon quickly.

Responsibility	Claranet	You
Contact information: Provide contact details of the security consultants involved in the service.	✓	
Contact information: Provide contact details of the primary contact responsible for the delivery of the consultancy. This contact will be responsible for arranging access to stakeholders and site locations to support the delivery of the consultancy.		✓
Scheduling: Inform Claranet Cyber Security of any changes to the dates, contact details or scope as early as possible. Changes to dates and scope may result in additional costs (see **Appendix**).		✓
Scheduling: Inform you in a timely manner of any changes to dates or to the security consultants involved in the delivery of the testing activity.	✓	

Agreement and confirmation

At the conclusion of this phase, the scope of the estate involved, the design of the consultancy, and pricing have all been confirmed and agreed.

Responsibility	Claranet	You
Order: Once completed, you will agree the Scoping Document, the Statement of Work, the Master Services Agreement, and the Sales Order Form in order that Claranet can begin the consultancy on the agreed dates.		✓

Consultancy

Commencement of the engagement

The engagement will begin on the dates agreed. This will be against the objectives and/or tasks within the Statement of Work.

Responsibility	Claranet	You
Engagement start: Claranet Cyber Security's security consultant will commence the agreement on the agreed date, either onsite or remotely via Microsoft Teams, or another suitable mechanism if Microsoft Teams is not suitable.	✓	
Plan: Upon commencement of the consultancy, the security consultant, together with the 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.	✓	✓
Supply supporting documentation/information: Ensure that the security consultant has all the necessary information needed to perform the consultancy effectively.		✓
Arrange site visits: Ensure that the security consultant has access to all sites required to complete the engagement.		✓
Arrange internal meetings: Arrange for access to all stakeholders required to complete the engagement.		✓
Provide continuous support: To limit the possibility of Scope Creep or an incomplete report, the consultant will need to be supported for the duration of the consultancy.		✓
Non-compliance: If, during the consultancy, a non-compliance determination is found; the primary contact will need to indicate if a non-compliant ROC/AOC/SAQ is required. Otherwise, a summary email or spreadsheet of non-conformities will be issued.		✓

Location of consultancy

Security consultants will conduct the consultancy from a location agreed during the **Scope** and **Prepare for consultancy** stages and as outlined in the Statement of Work. PCI Consultancy will often require additional site visits which will often be determined during the consultancy, although an indication of areas and the number of sites per area will be communicated during the Scope and Prepare for consultancy stages.

For 'Assessment' services, pre-arranging specific site locations is not carried out and these will be identified during sampling as part of the consultancy.

Timing of the consultancy

Consultancy is typically completed between 09.00hrs and 17.30 hrs, Monday to Friday. For onsite visits, if this needs to be different, based upon stakeholder working patterns, this should be discussed during the **Scope** and **Prepare for consultancy** stages, or can be discussed during the start of the consultancy, if agreeable by the security consultant allocated.

Methodology

Unless Claranet Cyber Security has agreed a bespoke service offering, each PCI Consultancy service has a specific methodology associated with it. The specific methodology for each service offering is detailed within the specific methodology that will be shared as part of the sales process.

Responsibility	Claranet	You
Sharing the documented methodology: Unless delivering bespoke consultancy, Claranet Cyber Security will share the latest methodology for the service being consumed.	✓	
Objective/task driven consultancy: Deliver consultancy in accordance with, and bounded by, the Scoping Document and Statement of Work.	✓	

Handling of sensitive data

During the consultancy, Security Consultants may come into contact with sensitive data. Consultant's laptops are encrypted to a minimum of AES 256 encryption to protect any data or information we encounter.

Sensitive data will typically flow from the client to the security consultant for review purposes as part delivery of the consultancy. Claranet Cyber Security will support the client's requirements for this communication flow.

Responsibility	Claranet	You
Sensitive data: Act in accordance with the Claranet Cyber Security practice for handling of your sensitive data and general best business practice. Security consultants will, where possible, avoid coming into the possession of Personally Identifiable Information.	✓	
Sensitive data transfers: Potentially sensitive data will need to be shared with the security consultant whilst fulfilling the consultancy. The primary contact will need to agree on a suitably secure mechanism for transfer said data.		✓

Review

Reporting

Once the consultancy is complete, a PCI Consultancy Report is produced which includes:

- Executive summary
- Graphical summary (some services)
- 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

Some services, i.e., Gap Analysis, will provide a graphical summary which may indicate the number of PCI DSS requirements that are found to be in place and the number found to not be in place.

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 which PCI Consultancy is taken, or specific objectives where bespoke consultancy is provided.

Quality Assurance

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

It is then sent directly to your nominated contact(s) in the Scoping Document by the pre-agreed and appropriately secure method.

Full final reports are completed within 10 working days, though larger projects or where there are delays, agreed by the security consultant, in receiving information during the consultancy stage, may take longer. Additionally,

for assessments, the reports may be delayed up to 1 month after the scheduled consultancy days if there is a requirement for the reports (SAQs/ROCs/AOCs) to be signed off when the previous compliance reports expire. Where this is the case if it can be identified and communicated during the **scope phase**. Where results are required by a specific date, this needs to be agreed during the **scope phase**.

Remediation

When performing PCI Consultancy involving PCI DSS assessment activities, and non-compliant requirements are identified, the security consultant will allow remediation during the consultancy; however, reviewing newly supplied evidence will only be completed providing there is time during the agreed consultancy period.

Where consultancy results in a non-compliant PCI DSS assessment, the security consultant will supply details of the non-compliant issues and remediation advice as an email or within a spreadsheet. If a non-compliant SAQ/ROC or AOC is required, this needs to be communicated during the consultancy stage.

Where remediation evidence cannot be reviewed during the consultancy which results in a passing assessment, an additional cost, based upon the number of days to review outstanding evidence and update reports will be required and will be communicated after the consultancy has completed.

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, you must inform Claranet Cyber Security as early as possible so this can be accommodated. We will make all reasonable endeavours to accommodate the request and will discuss these with you at the **Scoping** and **Prepare for testing** stage. This is to ensure that adequate resource can be assigned to the production and QA of your reports for the specified time.

Re-assessment

Following a period of remediation, there may be a requirement for a security consultant to re-assess evidence to validate remediated requirements are deemed in place. This is a chargeable exercise and the number of days required to complete a re-assessment activity will be discussed at the end of the initial consultancy period.

Re-assessments must be completed within one calendar month of the end of the initial consultancy, otherwise a full assessment may be required since original evidence collected will become stale. If there are technical or business constraints which are likely to cause the remediation to take longer than one calendar month, this needs to be discussed prior to booking the re-assessment. Claranet Cyber Security has some discretion over this time-period and may be able to accommodate a slight extension.

Responsibility	Claranet	You
Accuracy of reporting: Apply a rigorous Quality Assurance process to ensure that the results reported are accurate.	✓	
Delivery of reports: Deliver a report as soon as possible following the completion of the consultancy. This will contain an executive summary and consultancy findings.	✓	
Following up reports: Make available security consultants. This needs to be discussed during the **Scope** and **Prepare for consultancy** stages as this needs to be accounted for in the Scope of Work and needs to be factored into resourcing and pricing.	✓	
Re-assessment: Discuss re-assessment requirements with the primary contact during the consultancy. Re-assessment may be required if the outcome of assessment activities results in a non-compliant status.	✓	
Re-assessment: Book additional re-assessment days to cover re-assessment activities.		✓
Receiving reports: Provide contact details (email and mobile phone number) for the individual who is to receive the report. This must be provided at the outset of the testing and should be included in the Scoping Document. You will also maintain the list of current contacts in the event of changes from the original list.		✓

Feedback

Claranet strives to continuously improve the services offered to its customers and one of the main ways that we achieve that is by listening. We would love your feedback on how we performed before, during and after the engagement and any suggestions you may have to help us to improve the service. Your opinions are important to us so please complete the short feedback survey below:

Customer Feedback Form

Appendix

Service terminology

Throughout the document or in association with it, a number of terms have been used. These can be found in the general description below.

- **AOC**: Stands for Attestation of Compliance, which is a PCI SSC issued form completed after an assessment whereby an entity (and where applicable a QSA) will attest to the accuracy and validity of the assessment.
- **Assurance Team**: This is the Claranet Cyber Security team that delivers consultancy relating to governance, risk and compliance.
- **CDE**: Stands for Cardholder Data Environment, which is the environment in scope for the PCI DSS. This consist of the environment that stores, processes or transmits CHD or "connected to" systems.
- **CHD**: Stands for Cardholder Data, which is a term used to describe, cardholder data which consists, at a minimum, of the full PAN.
- **Master Services Agreement (MSA)**: This is a legal document provided by Claranet to the client which sets out and explains the legal conditions of the sale.
- **PAN**: Stands for Primary Account Number, which is the long card number across the front of a debit or credit card. This number is a unique identifier that identifies that specific card and cardholder.
- **Personally Identifiable Information**: Can also be referred to as PII,
- **PCI Consultancy**: This is a term used to describe consultancy services related to the payment card industry; for example, the PCI DSS.
- **PCI Consultancy Report**: This is the reporting output from the PCI Consultancy service delivered.
- **QSA**: Stands for Qualified Security Assessor, which is an individual working for a QSA Company that has successfully passed the QSA requirements, training, and exam.
- **Quality Assurance**: This is a process followed to check the quality of client reports before they are issued.
- **ROC**: Stands for Report on Compliance, which is a PCI SSC issued report that is completed by a QSA upon completion of an onsite PCI DSS assessment.
- **Sales Order Form**: This is the quotation document containing pricing and other details of the service being purchased. The signing of this quotation document by the client confirms the purchase contract between both parties.

- **SAQ**: Stands for Self-Assessment Questionnaire, which is the PCI Security Standards Council (PCI SSC) issued forms that can be submitted to report on PCI DSS compliance.
- **Scope Creep**: This is a term used when the scope of an engagement is deemed insufficient which will often result in additional days of consultancy.
- **Scoping Document**: This is a document completed by the client and provided to Claranet containing the information related to the assessment necessary for a Statement of Work and quotation to be produced.
- **Statement of Work**: Can also be referred to as SOW, this is a document completed by Claranet and provided to the client at the conclusion of the scope stage, which confirms the scope of the engagement and the activities that will take place during the engagement.

The components of the PCI Consultancy portfolio are supported by a set of documented methodologies, which are available on request.

Fees, payment and legal

Fees payable under this Contract will be invoiced on delivery of the PCI Consultancy report(s) or, if no report is to be provided, on completion of the consultancy.

If ordered days not paid for up-front are not used within 12 months, then Claranet Cyber Security will invoice the days. You will then have 6 months to schedule the days.

Delays and cancellations

Immediately following the agreement of dates for the PCI Consultancy service to begin and the receipt of the purchase order, Claranet Cyber Security will start to allocate resources and facilities and will therefore commit to any third party expenditure to fulfil its contractual commitments. Claranet Cyber Security may at its absolute discretion allow the PCI Consultancy to be re-scheduled or cancelled. If this occurs, you agree that you are committed to paying Claranet Cyber Security a proportion of the fees as pre-estimated liquidated damages. In the case of late notice rescheduling, this fee will be in addition to the full price for the engagement which will be invoiced upon delivery of the PCI Consultancy Report. This will reflect the losses which Claranet Cyber Security will incur because of the cancellation or re-scheduling.

These proportions are as follows:

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 security consultant allocated to your PCI consultancy 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 Cyber Security will endeavour to minimise the impact on the delivery of the results.

Travelling

For onsite work, account managers and security consultants will plan the schedule of the engagement to take into account travel time. Clients are not normally charged for time incurred during travelling (only the cost of the travel), to maximise the available consultancy time, some engagements may start at any time up to midday. Where this is the case, your account manager will discuss and agree the options that are available. Where travel delays are incurred the Security Consultant will contact you to provide an estimated time of arrival. Where possible the security consultant will make up any time lost by travel delays during the engagement.

Billing

Where you order PCI consultancy day units and do not allocate or use these within twelve months, Claranet Cyber Security will invoice you for these days at our convenience on or about the twelfth month, whether or not you allocate the days at that time.

Expenses

Expenses are charged at cost for travel, accommodation and sustenance where onsite work is required. Your account manager can provide you with an estimate of any likely expenses during the **Scope** stage. To ensure accuracy and the lowest costs possible, expenses are charged upon completion of the consultancy unless otherwise agreed.

Scope changes

If, prior to the consultancy or during the consultancy, the scope changes, this may incur an additional cost.

Scope changes can occur if additional information regarding an organisations payment environment come to light, or any segmentation techniques are deemed insufficient to remote systems from the scope of the PCI DSS assessment.

Legal obligations

By signing the Sales Order form:

1. You hereby give permission to Claranet Cyber Security to all information required in pursuant to the Statement of Work;
2. You confirm that you have obtained all consents required from data subjects to enable personal data (as defined in applicable data protection legislation) to be disclosed to Claranet Cyber Security to the extent required to carry out the PCI Consultancy;
3. You agree that, where the PCI Consultancy is to take place on your premises, you shall ensure that a suitable working environment is provided for the Claranet Cyber Security consultant.
4. You agree to provide Claranet Cyber Security with at least one employee who has substantial computer systems, network and project management experience of your information system to act as liaison between you and Claranet Cyber Security.
5. You agree to co-operate with Claranet Cyber Security and to provide it promptly with such information about your CDE as are reasonably required by Claranet Cyber Security to perform the PCI Consultancy.
6. You confirm that, where the PCI Consultancy is taking place on your premises, the premises are safe in line with current Covid-19 guidelines, suitable and reasonable to accommodate Claranet Cyber Security's security consultant.
7. You agree that copyright in the PCI Consultancy Report(s) received by you in relation to the PCI Consultancy shall remain the property of Claranet Cyber Security, and that Claranet Cyber Security, upon receipt of payment in full, hereby grants you a non-exclusive, non-transferable licence to copy and use the contents of those PCI Consultancy Reports for your own internal purposes only.