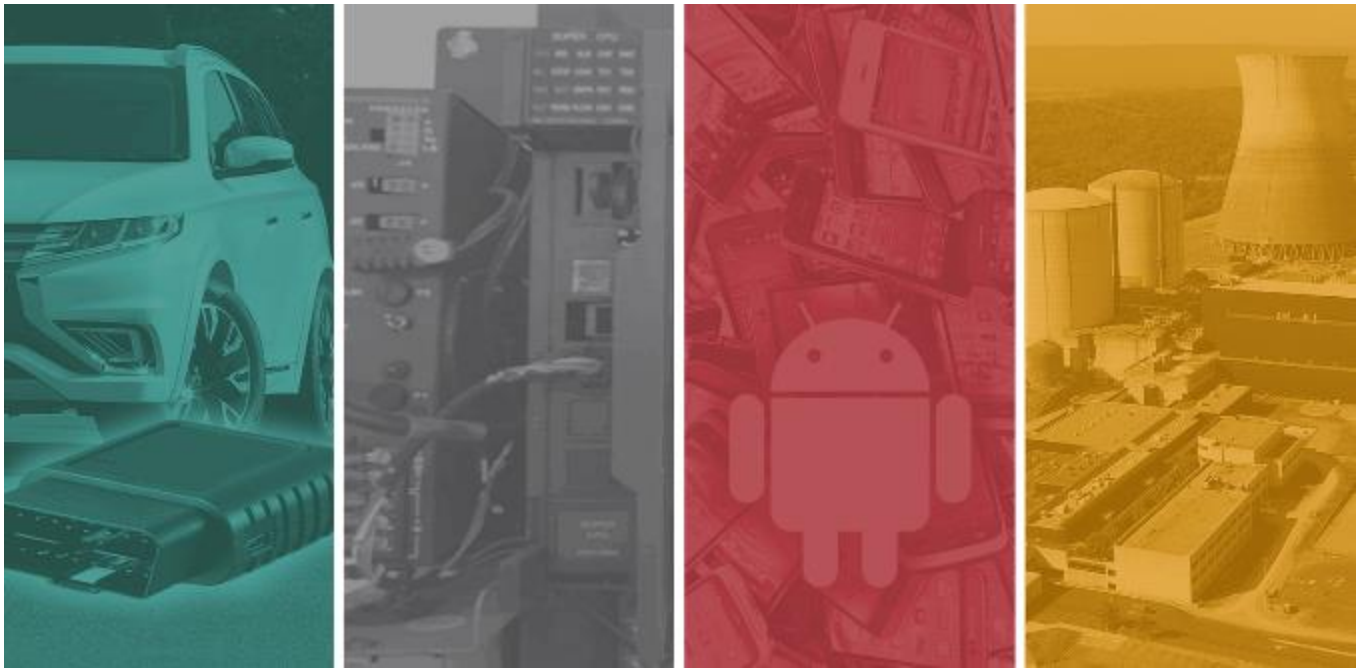
PTP Cyber Consultancy – 'Comply' Service Definition Document

G-Cloud – 14 (RM1557.14) Lot 3 Cloud Support, Security Services– Security Services



Version 1.0
26 April 2024

Table of Contents

1. PTP Consultancy Services

1.1. PTP Consultancy Services

This document sets out the PTP 'Comply' Consultancy Services. Our PTP Consultancy services can be purchased individually or grouped across the range of Design, Discover, Improve & Comply services based on our clients' specific needs.

Design	• Architecture - Best Practice	Improve	• DFIR - Business continuity planning
Design	• Architecture - Cloud Security Controls	Improve	• DFIR - Incident response plan
Design	• Architecture - Secure Development	Improve	• DFIR - Tabletop exercise / simulation
Discover	• Cloud - Security Support (Azure & AWS)	Improve	• 3rd Party Supplier Assurance
Discover	• Cloud - M365 review	Improve	• 3rd Party - Vendor Selection
Discover	• Cyber Security - Gap analysis	**Comply**	• **Cyber Essentials & Essentials Plus - Consultancy, Review and Assessment**
Discover	• Cyber Security - Maturity Assessment	**Comply**	• **PCI - ASV Scanning**
Discover	• PCI - Scoping Workshop	**Comply**	• **PCI - Card data scanning**
Improve	• vCISO - Policy Development	**Comply**	• **PCI - Level 1 ROC assessment**
Improve	• vCISO - Security Posture Improvement	**Comply**	• **PCI - SAQ assessment**
Improve	• Cyber Security - Certification preparation		
Improve	• Cloud - M365 Enhancement		

2. PTPs approach to Working Together and Pricing

Every consultancy project PTP delivers is custom managed. From initial scoping through to debrief we will ensure the right approach and people are being utilised.

For a project to be successful PTP needs to achieve the goals set out at the beginning. This means we need to understand more than just what the requirement is. We need to understand where the requirement has come from, what is the business hoping to achieve from this project and why?

It's important to set clear expectations, ensure the scope is accurate and any risks, dependencies or limitations are understood in advance.

PTP typical working model:

- **Dedicated Account Manager:**
  - PTP will allocate a dedicated account manager as a central point of contact for the duration of the relationship.
- **Initial Consultation:**
  - For each new consultancy engagement, PTP will initiate a conversation via email and/or call to understand your service requirements. This serves as the introduction call.
- **Scope of Works (SOW) Creation:**
  - A PTP technical consultant will review all relevant information and create a detailed Scope of Works (SOW). This document will include any necessary prerequisites.
- **Proposal and SOW Delivery:**
  - PTP will send a comprehensive Proposal/SOW, specifying:
    - Duration
    - Cost
    - Grade of consultant required
    - Proposed dates (if already discussed)
- **Pricing Calculation:**
  - Pricing will be determined based on the number of days required to deliver the services using the service day rates.
- **Acceptance of Proposal / SOW**
  - Upon acceptance of the SOW, delivery dates are agreed and scheduled.
- **Authorisation and pre-requisite information**
  - PTP will send an Authorisation form for signature and return.
- **Pre engagement Kick off Call**
  - PTP will host a pre-engagement call to discuss the engagement and introduce the team.
- **PTP undertakes the required services.**

3. Consultancy Comply Services

- Cyber Essentials & Essentials Plus - Consultancy, Review and Assessment
- PCI - ASV Scanning
- PCI - Card data scanning
- PCI - Level 1 ROC assessment
- PCI - SAQ assessment

3.1. Cyber Essentials & Essentials Plus - Consultancy, Review and Assessment

Consultancy

PTP will provide a spreadsheet version of the Cyber Essentials questionnaire via email.

The approach will consist of:

- Customer completes an initial 'first pass' of the spreadsheet and the responses where possible. Any questions which are unclear should be left blank for review.
- The PTP consultant will review the initial spreadsheet version responses and annotate in preparation for a review interview.
- Interview between customer and PTP to validate responses and provide additions where required.
- PTP will then complete a final run through of the responses and check against the current marking guide to confirm a likely passing status.
- Assuming no remediation is required, a final wash up call will be held to agree next steps for client and arrange Pervade Portal access.
- If remediation is required a statement of work (SoW) will be produced, that PTP can provide support consultancy if required at an additional cost to be agreed.

Cyber Essentials

The client proceeds with completion of the questionnaire via Pervade Portal and provides the scope and information there.

Notes

- A window of 48 business hours is available for amending CE Questionnaires if a failure is attained.
- If the organisation fails after 2 attempts, they must wait 1 month before re-applying.

Cyber Essentials - PLUS

Once a pass confirmation is attained, the client will proceed with appropriate external and internal testing to further validate compliance with Cyber Essentials and, therefore, attaining a Plus Status.

Notes

- CE Plus must be undertaken within 3 months of passing CE.
- The organisation being tested for CE Plus must have already achieved the Cyber Essentials self-assessment and the scope for the self-assessment must be the same as the scope for the CE Plus test.
- A window of 30 days is available for remediation and retesting after an initial CE Plus fail. The assessor must retest any specific issue identified and confirm it is resolved before issuing a certificate.
- If the client takes longer to remediate an issue, the whole CE Plus assessment must be carried out again by the assessor.

3.2. PCI ASV Scanning

Approved Scanning Vendor (ASV) scans are a requirement of the PCI DSS standard. Requirement 11.3.2 mandates that external vulnerability scans are required to be performed by a PCI SSC ASV at least once every three months.

As per the ASV Program guide:

"For the purpose of ASV scanning, PCI DSS requires vulnerability scanning at least once every three months of all externally accessible (Internet-facing) system components owned or utilized by the scan customer that are part of the cardholder data environment (CDE), as well as any externally facing system component that may provide access to the CDE.

In addition to providing the ASV with all external-facing IP addresses, the scan customer must also supply all fully qualified domain names (FQDN) and other unique entryways into system components for the entire in-scope infrastructure including, but not limited to:

- Domains for web servers
- Domains for mail servers
- Domains used in name-based virtual hosting
- Web server URLs to "hidden" directories that cannot be reached by crawling the website from
- the home page
- Any other public-facing hosts, virtual hosts, domains or domain aliases

The scan customer must define and attest to its scan scope prior to the ASV finalizing the scan report. The scan customer is ultimately responsible for defining the appropriate scope of the external vulnerability scan and must provide all Internet-facing components, IP addresses and/or ranges to the ASV. If an account data compromise occurs via an externally-facing system component not included in the scan scope, the scan customer is responsible."

PTPs Scanning services includes:

Onboarding:

• Working with our clients to define the correct scope of IP ranges and FQDNs for scans.
• Setup and configure tooling to run automated scans based on the scope.

PTP works with Sectigo, and their ASV scanning product Hacker Guardian. This utilises the Qualys Cloud scanning Engine.

All network traffic will originate from the following cloud service IP Address ranges:
• 64.39.96.0/20 (64.39.96.1-64.39.111.254)
• 139.87.112.0/23 (139.87.112.1-139.87.113.255)

Defence mechanisms such as IDS/IPS should whitelist these source address ranges to prevent scan interference during testing.

License costs include unlimited scans against the nominated scope range.

3.3. Card Data Scanning

PCI customers are required to define the scope of their CDE (Card Holder Data Environment), by understanding where Credit card data is present / not present. To determine this, Data Loss Prevention (DLP) tools can be used to scan for the presence of credit card data.

One method to achieve this, is through scanning tools that can automatically crawl:

- Local and network file systems
- Database instances
- Email services (either local outlook clients or online mailbox services

The above provides clients with the following:

- Proving an absence of card data outside the segregated environment, through sampling scans across the business network.
- Identifying presence of card data in the PCI environment, to support documentation such as data flows and validate that card data only resides where expected.

Ket Points

- Software tools used are locked to named devices and may have other restrictions such as local server agents not being able to scan network drives. Scoping needs to identify all resource types to ensure sufficient licenses are available.
- The tools used can typically identify other data types such as Personally Identifiable Information (PII), which could be used to support ICO/GDPR data mapping activities.
- Enterprise versions of software can be deployed from a central server and operated on an automated basis for larger environments.

3.4. PCI - Level 1 ROC assessment

Customers with over six million total annual transactions across all payment channels, are required to complete a Qualified Security Assessor led assessment. To support the assessment process, an onsite or remote assessment will be completed to review applicable requirements. There are some instances, such as the physical security review of a data centre, where an onsite review day may be required.

Reviews are typical across one or more of the following payment channels:

- **E-commerce** - websites containing a payment function, that is either hosted by the customer or redirected to a payment processor.
- **MOTO** - Mail Order (Order forms containing card details)/Telephone Order (Full or ad-hoc call center functions. This can be a single machine in a finance office for occasional over the phone payments only).
- **Customer present** - retail environments, where the customer will provide their card and operate a card machine.

The reporting is produced following onsite and remote reviews for all in scope payment channels, based on Merchant IDs owned.

The assessment will also consider any Third-Party Service Providers (TPSPs) that provide outsourced or supporting services for those payment channels.

Pen Test Partners (PTP) will provide PCI QSA services to complete the following stages:

Stage One (Optional)
Prior to a final assessment, complete a high-level workshop to review in scope controls. The purpose of this activity is to ensure the business has correctly scoped their payment channels, and appropriate controls are in place. This stage considers:

- What is in place now and could be assessed. Typically, technical controls are in place (such as password complexity / unique user IDs / patching etc.) but some supporting documentation and processes may need to be remediated before final assessment.

- Agree dates for completion of any remediation items prior the onsite assessment being scheduled.

Stage Two
Consists of several activities:

- Review of the payment channel environment(s) and capture screenshots / log files etc. as evidence. PTP will also complete interviews with key staff to support the assessment.
- Requests for any documentation, to be stored with the report and answer documentation specific controls.
- (offline) – PTP compile the detailed responses in the ROC report, including overview of the environment and creating any required diagrams / data flows in Visio to go in the report.

- (offline) – Entire report is QA reviewed by another QSA to confirm report is defensible and accurate (a PCI SSC requirement)
- PTP finally sends over an AOC (Attestation of Compliance) and ROC report for <Full Client Name> to review and sign, and PTP to countersign.

3.5. PCI - SAQ assessment

Customers with less than 6M total annual transactions (across all payment channels), are required to complete a specific SAQ (Self-Assessment Questionnaire):

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS validated third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. **Not applicable to face-to-face channels.**
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. **Applicable only to e-commerce channels.**
B	Merchants using only: • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. **Not applicable to e-commerce channels.**
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. **Not applicable to e-commerce channels.**
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. **Not applicable to e-commerce channels.**
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. **Not applicable to e-commerce channels.**
P2PE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. **Not applicable to e-commerce channels.**
D	SAQ D for Merchants: All merchants not included in descriptions for the above SAQ types.
	SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete a SAQ.

Key Points:

- Multiple SAQs can be submitted to the acquiring bank (one per payment channel). This is usually clearer to document.
- SAQ support is completed on one of two levels:
    - Consultancy defines the correct scope and identifies the applicable SAQs from the list above. Customer is responsible for evidencing the applicable controls are in place.
    - Consultancy completes the step above, and in addition will sample controls.

4.0. Introduction to PTP

Pen Test Partners LLP is focussed on delivering innovative and meaningful penetration testing, DFIR and Consultancy services. It's a simple mandate, and one that we have built our business and reputation with.

Why choose Pen Test Partners?

Established in June 2010, we have consultants with a vast range of skills and experience, some with extremely niche skills.

As an entire company we know our stuff and we'll work at your pace.

We research, test, and assure a lot of interesting and complex things!

We've provided testing and assurance for all sorts of things; ships at sea, international finance infrastructure, mobile apps for smart toys, airplane systems and avionics, power stations and critical national infrastructure, automotive and telematics, mobile banking apps, physical security, cloud services to rail infrastructure.

Our Credentials

PTP are a CREST, CBEST, ASSURE, STAR, CSIR, CHECK, Tigerscheme, PCI QSA, ISO27001, Cyber Essentials/+ accredited ; this ensures the highest quality of testing.

All PTP staff are vetted prior to commencement of employment in line with British Standard 7858 Clearance Service and through the Disclosure and Barring Service (DBS). National Vetting Solutions. All our security consultants are a minimum of SC cleared.

What we provide

Responsiveness

We are recognised as being extremely responsive. We can begin an engagement with as little as 24 hours' notice.

Follow-up

One of the reasons we have such loyal clients is the availability our consultants have for follow-up work.

Ongoing guidance

Once an engagement is over… It's never truly over, there will always be questions, queries, and advice needed, so we make a point of always being available post engagement.

Our Reputation

The BBC and other news agencies often contact us to comment on the latest cyber news.

We are frequently called upon to provide keynotes at events such as BSides, TED talks, InfoSecurity Europe and the US Chamber of commerce.

We can’t name names, but our clients come from a wide range of verticals and sizes including: Automotive, Banking, Education, Engineering, Energy, Oil & Gas, FinTech, Government, Healthcare, Manufacturing, Retail, Telco’s, Insurance, Legal, Transport and Finance.