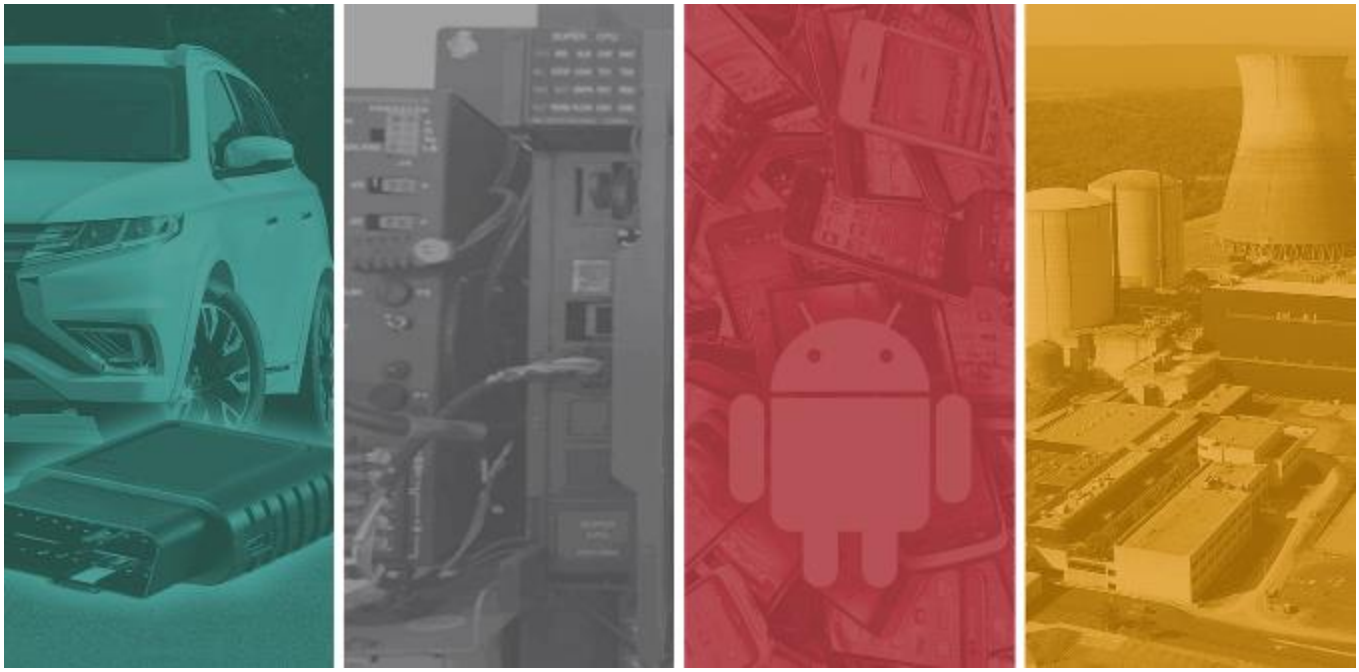
PEN TEST PARTNERS

PTP Cyber Consultancy – 'Secure by Design' 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

info@pentestpartners.com +44 (0)20 3095 0500 @PenTestPartners PenTestPartnersLLP

1. PTP Consultancy Services

1.1. PTP Consultancy Services

This document sets out the PTP 'Secure by Design' 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 a 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 Design Services

- Architecture - Best Practice
- Architecture - Cloud Security Controls
- Architecture - Secure Development

3.1. **Architecture** – Best Practice

At the design stage, PTP conduct security reviews including:

- Review of documented security architecture / design of new systems
- Workshop proposed design changes or service additions to a current environment

The intention is to identify controls or in some cases alterations to the design, to support specific legal, regulatory, or contractual requirements the customer needs to meet. Examples include:

- Consideration of PCI requirements, where an environment will support credit card payments
- Meeting the customers client expectations for security to support an RFP or new service provision
- Specific design considerations to support secure implementation of new cloud environments
- Review of the customers CI/CD (Continuous Integration / Continuous Development) pipeline and supporting processes, to ensure the follow best practice.

3.2. Architecture – Cloud Security Controls

PTP review of security principles outlined by the National Cyber Security Centre (NCSC) in their NCSC Controls guidance (The cloud security principles - NCSC.GOV.UK). The review is set through a comprehensive questionnaire and follow-up report.

The controls are a set of Cloud Security best practice, intended to mitigate common attacks against systems and services.

- Principle 1: Data in transit protection
- Principle 2: Asset protection and resilience
- Principle 3: Separation between customers
- Principle 4: Governance framework
- Principle 5: Operational security
- Principle 6: Personnel security
- Principle 7: Secure development
- Principle 8: Supply chain security

- Principle 9. Secure user management
- Principle 10: Identity and authentication
- Principle 11: External interface protection
- Principle 12: Secure service administration
- Principle 13: Audit information and alerting for customers
- Principle 14: Secure use of the service

3.3. Architecture – Secure Development

PTP will review of the 5 key security principles outlined by the National Cyber Security Centre (NCSC) in their NCSC Secure Design Principles (Secure design principles - NCSC.GOV.UK).

The controls are a set of Five principles for the design of cyber secure systems:

- Establish the context before designing a system
- Make compromise difficult
- Make disruption difficult
- Make compromise detection easier
- Reduce the impact of compromise

Key Points:

- Time needed for initial questionnaire depends on team size and complexity of cloud environment being reviewed.
- The initial approach for the assessment is a based general audit practice:
  - Review of current documentation and processes.
  - Interviews with staff at management and front-line levels.
  - Sampling of controls and evidence gathering to confirm effectiveness and coverage.
- PTP will provide a thorough report, detailing findings, and recommendations to improve the design and security of the solution.

3.4. Introduction to PTP

Pen Test Partners LLP is focussed on delivering innovative and meaningful penetration testing. 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've got 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, NCSC CIRL2, 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.