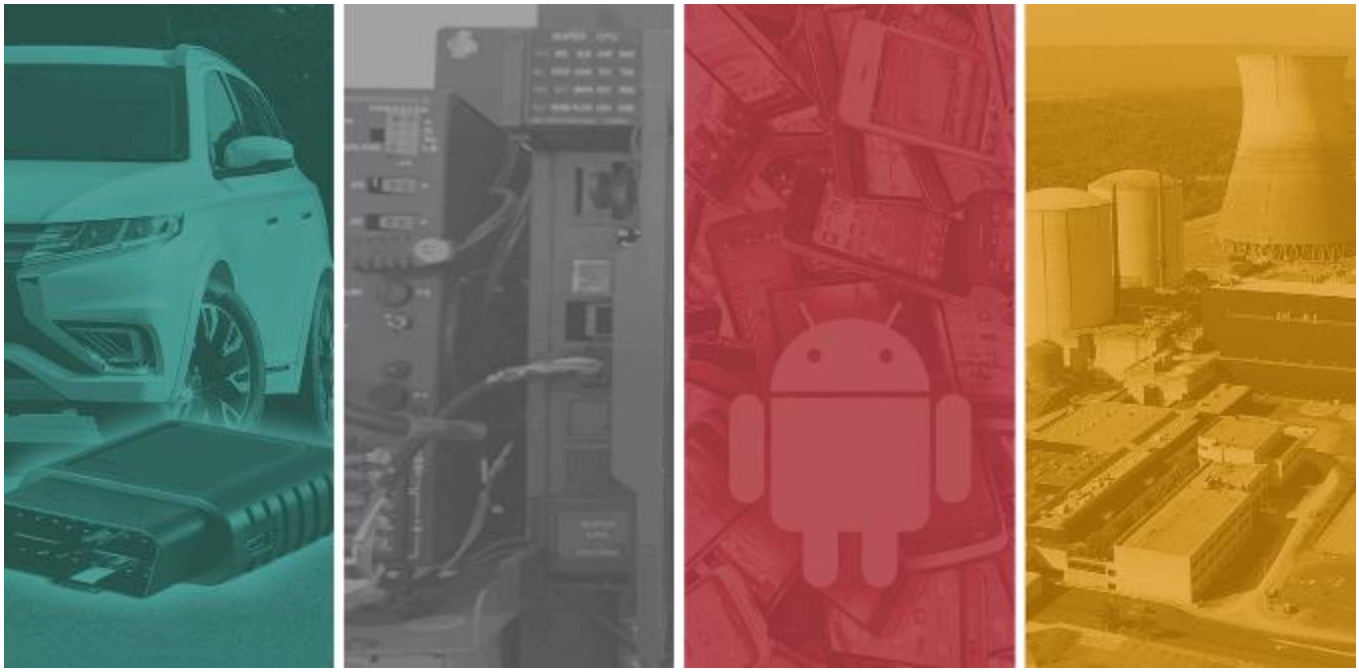
PEN TEST PARTNERS

PTP Cyber Consultancy – 'Improve' 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 'Improve' 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 we deliver 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 we need 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 scope is accurate and any risks, dependencies or limitations understood in advance.

PTP typical working model:

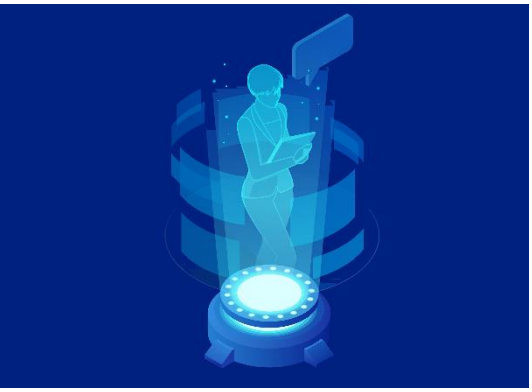
- **Dedicated Account Manager:**
  - PTP will allocate a dedicated account manager as a central point of contact for the duration of the relationship.
- **Initial Consultation:**
  - For each new consultancy engagement, PTP will initiate a conversation via email and/or call to understand your service 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 Improve Services

- vCISO - Policy Development
- vCISO - Security Posture Improvement
- Cyber Security - Certification preparation
- Cloud - M365 Enhancement
- DFIR - Business continuity planning
- DFIR - Incident response plan
- DFIR - Tabletop exercise / simulation
- 3rd Party Supplier Assurance
- 3rd Party - Vendor Selection

Contact us today:
info@pentestpartners.com
+44 (0)20 3095 0500

vCISO:
Policy Development



Why do clients need this?

PTP's Virtual CISO Policy Development service is designed to help clients develop and improve information security policies and standard operating procedures, to support information security management systems.

PTP's consultants identify opportunities for improvement with existing policies, implement enhancements, and develop new policies that are tailored to clients' requirements. Policy improvement will help update, modify or simplify existing and legacy documents.

How does it work?

The time required to complete the engagement will depend on how much support you need.

Our consultants will work with you to scope the program of work based on their business requirements.

We can map the development and enhancement of policies to specific regulatory requirements and compliance standards.

We review existing or legacy policies and identify opportunities for improvement.

We then implement enhancements based on the client's requirements and objectives.

Key features

PTP's consultants work with clients to determine requirements and objectives. The goal may be to simply improve the organisation's information security management system or could be related to a larger body of work, such as achieving formal certification.

Existing or legacy policies will be thoroughly reviewed to identify opportunities for improvement.

PTP's consultants will then assist to implement recommendations and enhancements.

New policies will be developed and tailored based on the requirements and information security management systems. Information security policies will be mapped to clients' objectives as well as regulatory requirements and standards.

Problems it solves

This service can be used to complement existing internal information security capabilities.

Provides clients with expert help and guidance where the necessary in-house skills and expertise is not currently available.

Helps develop a solid foundation upon which an information security program can be built.

Ensures organisations are compliant with legal, regulator, and formal certification requirements.

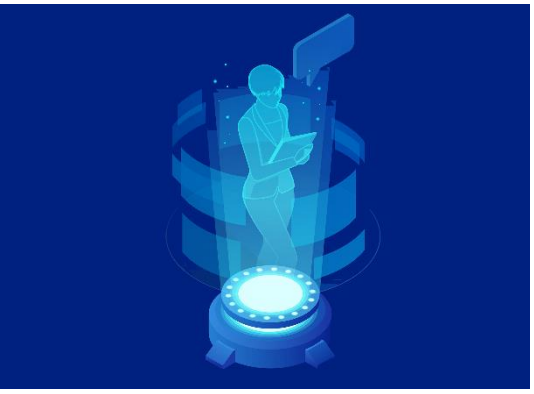
Protects organisations by outlining the requirements to which business stakeholders must adhere and facilitates accountability.

Helps businesses formalise and direct their information security program.

PEN TEST PARTNERS

Contact us today:
info@pentestpartners.com
+44 (0)20 3095 0500

vCISO:
Security Posture Improvement



What's involved?

This service offers ongoing support to help enhance clients security posture, following a review where opportunities for improvement are identified.

PTP will work with clients to complete discreet pieces of work as required. This may include a defined project over several days or ongoing support through emails and short calls where the client is billed on a half-day basis.

PTP helps clients identify, plan, implement, and track changes as required, to continually improve their information security program.

Why do clients need this?

Our Security Posture Improvement service is designed to help clients develop and improve the organisation's security posture, using a review in which opportunities for improvement are identified.

This may include discrete elements of work completed over a set number of days, or ongoing support as clients look to improve the maturity posture over a longer period of time.

What can clients expect?

The service provides organisations with expert help and guidance where the necessary in-house skills and expertise are not available.

It identifies and addresses opportunities for improvement within information security management systems to further enhance security postures.

It supports newer or less mature organisations to develop an information security management system.

It directs and aligns security programs to specific standards and frameworks, beneficial to organisations seeking to obtain formal certification.

It helps organisations implement the controls necessary to ensure compliance with specific legal and regulatory requirements.

How does it work?

Clients usually engage PTP for this service following a review of their information security posture.

The time required to complete the engagement will depend on how much support clients require.

PTP's consultants will work to scope the program of work based on the specific objectives and requirements of the security program.

A set number of support days are allocated to specific projects, or support can be provided on an ongoing basis.

PEN TEST PARTNERS

Contact us today:
info@pentestpartners.com
+44 (0)20 3095 0500

Cyber Security:
Certification preparation

Problems it solves

Proactively identifies current maturity level of an organisation's information security posture and encompassing controls against a recognised framework.

This will help improve an organisation's information security program and supporting management systems

Identify and reduce information security related risks that the organisation faces

Identify gaps and areas for improvement in your information security posture

Ensures appropriate and efficient allocation of resources in advance of formal certification.

Why do clients need this?

This service is designed to guide clients on their journey toward formal certification for industry standards such as PCI DSS, ISO/IEC 27001, Cyber Essentials (CE), and CE Plus. Even if clients do not intend to achieve formal certification, they can still benefit from PTP's expertise by aligning their practices with these standards.

Clients can still use this service even if they do not intend to achieve formal certification but wish to work in line with a particular standard in the first instance. If required, we can also work with you and your certifying body through to full certification.

How does it work?

Tailored scoping: Thorough scoping exercises to understand the requirements.

Expert assessment: PTP assesses your people, processes, and technology against the required standard.

Roadmap development: Working closely with you, PTP creates a customised roadmap of remedial activities to prepare for formal certification.

Qualified consultants: PTP's consultants are highly qualified and experienced, adept at both certification preparation and internal information security program management.

Comprehensive support: beyond certification, we help you in various complementary areas, including policy development.

Trusted partnership: PTP serves as a reliable partner throughout your journey toward improving the security posture.

What do clients obtain?

Comprehensive guidance: PTP collaborate closely with you, providing step-by-step support throughout the certification process.

Flexible Approach: You can use the service regardless of your certification goals. Whether you need formal certification or simply want to align with a specific standard, PTP is here to help.

Holistic improvement: The focus extends beyond certification. PTP can help enhance an organisation's information security program and supporting management systems.

Gap analysis: PTP identify gaps and areas for improvement in your security posture.

Risk reduction: PTP pinpoints and mitigates the security related risks you face.

Resource Optimisation: By ensuring efficient resource allocation, PTP prepares you for certification in advance.

PEN TEST PARTNERS

Contact us today:
info@pentestpartners.com
+44 (0)20 3095 0500

Cloud:
Microsoft 365 Enhancement

What's involved?

Following the completion of a Microsoft 365 Review, PTP will aid the client in implementing the recommended security controls.

PTP's consultants can make the necessary configuration changes on behalf of the client, or can guide the client through the implementation of changes.

PTP can run training and development workshops with members of the client's team, this will provide personnel with the knowledge and skills necessary to maintain and further develop the security posture of the Microsoft 365 tenant into the future.

Why do clients need this?

This service helps organisations further enhance the security posture of their Microsoft 365 tenants once areas for improvement have been identified.

Our consultants work with clients to plan and implement security controls that address security requirements and gaps. Both technical and non-technical controls shall be addressed, such as insecure configurations and problematic processes.

What can clients expect?

This service helps clients take the next steps once opportunities for improvement have been identified.

PTP's consultants can implement controls and changes directly or help guide the client through the implementations.

Changes are identified, planned, implemented, and tracked in accordance with the client's change management policies and procedures.

PTP's consultants can run workshops which will provide personnel with the knowledge necessary to maintain and further improve the security posture of the Microsoft 365 tenant into the future.

How does it work?

Clients give PTP an internal account associated with administrative roles necessary to implement changes.

PTP works with clients to identify, plan, implement, and check configuration changes.

PTP can also schedule workshop sessions to review and implement configuration changes that address security gaps.

Problems it solves.

It helps directly fix Microsoft 365 security issues. It also helps less mature clients understand their Microsoft 365 estate better and reduces the likelihood and impact of a Microsoft 365 related security incident.

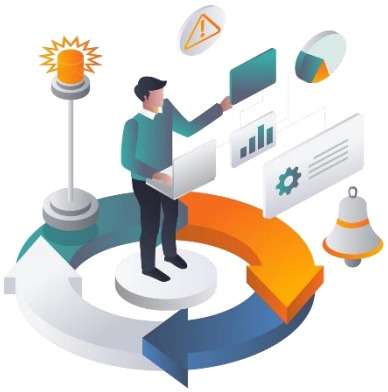
Clients can implement security features and controls through an existing license set which may have been unknown to the client.

Identify and address gaps in internal knowledgebase in relation to Microsoft 365 security.

PEN TEST PARTNERS

Contact us today:
info@pentestpartners.com
+44 (0)20 3095 0500

Business Continuity Planning



Hope for the best, plan for the worst

All organisations suffer incidents and unexpected events which have varying degrees of impact on their ability to operate. Having a robust Business Continuity Plan (BCP) will minimise the downtime and related costs.

A BCP also gives organisations a much better understanding of the information assets that support vital business functions. Having a BCP is one thing, but it also needs testing to ensure its effectiveness in the event of an incident.

Scope & objectives

PTP can help create a new BCP or further improve an existing BCP.

Our consultants will speak with key people in the organisation to review relevant systems and processes.

The findings and recommendations from the review will be presented and, then a roadmap of activities will be created to address the recommendations.

The goal is to enhance a client's understanding of the business assets and their value to the organisation, and critically to help you prioritise recovery.

Why do clients need this?

BCP is vital for all businesses, but can be a complex area that requires experience.

Ransomware is an ever present cyber threat, good BCP practices can make the difference between prolonged disruption and effective recovery.

A good BCP can mitigate risk and increase resilience to cyber-attack through a defence in depth approach.

Stakeholders and clients will have increased confidence in service continuity.

Resilience to cyber-attack and minimising downtime can create a competitive advantage.

Compliance with insurance and regulatory compliance.

BCP is about more than just IT. PTP is well aware of this and have the skills to help in all areas of business.

As more services move to a cloud 'XaaS' model, there are unique BCP considerations that must be made and accounted for.

As the threat landscape continues to evolve and cyber security incidents become more sophisticated and common, it is vital for an organisation to be able to respond and recover quickly.

This plan will minimise the effect of cyber security incidents by enabling quick responses to data breaches, quickly restoring critical systems and protecting assets, reputation and giving confidence to stakeholders.

PEN TEST PARTNERS

The BCP will encompass all areas of incident response and recovery including identifying assets, threat protection and detection, recovery, response, and lessons learned. The results from the PTP DFIR – Business Continuity Maturity review will be used to establish the areas that need to be addressed to create a robust BCP.

PTP can support the BCP development process in a number of areas:

Business Information Assets: PTP will work with clients to enhance the understanding of the business assets, their value to the organisation and their criticality to help prioritise recovery. Work may also be needed to understand primary assets and the supporting assets that are linked and would need to be included for successful recovery of a business service.

Drafting an initial BCP: engage with clients following an asset review, to create the starting documentation needed for a BCP. The BCP should be structured to allow elements to be devolved to business area leads for larger organisations.

Review of current BCP: reviewing existing documented process, and through interviews with business areas refine the process and the use of backup technologies to support business needs.

Defining and support testing: creating formalised testing plans that properly exercise the BCP, and generate improvement and actions from lessons learnt.

CREST

PEN TEST

STAR
Intelligence-led PT

STAR-FS
Intelligence-led PT

CSIR

OVS

CBEST

Assured Service Provider
in association with
National Cyber Security Centre
CHECK Penetration Testing

ASSURE

CYBER ESSENTIALS

bsi. ISO/IEC 27001 Information Security Management

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

PTP Services

Testing

- Penetration Testing – CHECK, CREST
- CREST STAR & CBEST
- Red Teaming
- Application Testing
- Infrastructure testing
- Mobile App & Device Testing
- Application Code Reviews
- Cloud Testing
- Social Engineering
- API & Web Services testing

Training

- Security Awareness Training
- Phishing Simulation & Training
- Hardware Hacking Workshops
- Developer Coding Training

PTP Tools

- PAPA Password Auditing Service

DFIR

- Digital Forensics
- Incident Response
- Mobile Device Forensics
- Incident Response Retainer
- Compromise Assessment

Specialist testing

- Maritime Cyber Security
- Rail Cyber Security
- Automotive
- Aviation & Aerospace
- IoT Security Testing
- ICS / OT / IIoT
- GBEST & TBEST

Consultancy

- PCI QSA
- ISO27001
- Virtual CISO
- General Security Consultancy
- Policy Creation and review

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

PEN TEST PARTNERS

Contact us today:
info@pentestpartners.com
+44 (0)20 3095 0500

DFIR:
Incident response plan

Problems it solves

All organisations suffer incidents and other unexpected events which can have a major impact on their ability to operate. A good incident response plan can minimise downtime and related costs.

It can help organisations gain a better understanding of the information assets that support vital business functions.

A comprehensive policy serves as an important foundation to an organisation's incident response capability and readiness.

It facilitates a coherent and uniform approach to cyber incident response across large and complex organisations.

Why do clients need this?

This is a service where PTP help clients develop their cyber incident response plans, this may include developing new plans from scratch or updating existing plans. Where a client is less mature, PTP may first help them develop their incident response policy before moving on to developing their incident response plans.

Plans and policies can be developed based on one core Security Incident Response Team that covers the whole organisation. A multi-SIRT approach can also be developed to include a set of core principles along with sub-company

What is included?

Assessment and enhancement:
PTP's consultants assesses your existing cyber incident response measures, to identify gaps and recommend improvements to align with industry best practices.

Customised strategies:
PTP guides you in developing tailored cyber incident response plans. These strategies address the escalating sophistication and frequency of threats, ensuring resilience.

Streamlined coordination:
PTP's plans serve as the core of your organisation's reaction to potential threats. They enable quick risk mitigation and damage minimisation, streamlining response efforts.

Compliance and risk management:
Regulators and insurers often mandate well-defined incident response procedures. PTP's services ensure compliance with data protection and cybersecurity laws.

How does it work?

You can benefit from this service as part of an IR Retainer, following a DFIR Maturity Review, or as a standalone project.

PTP undertakes scoping exercises to determine what level of policy, process, and documentation you already have in place.

PTP develops a standardised incident response policy based on best practice guidance from the NCSC.

PTP works with you to enhance your understanding of your business assets, and associated value to the organisation.

Assured Service Provider

in association with National Cyber Security Centre

Cyber Incident Response (Level 2)

PEN TEST PARTNERS

Contact us today:
info@pentestpartners.com
+44 (0)20 3095 0500

DFIR: Tabletop exercise

Why do clients need this?

The escalating threat of cyber-attacks is a serious concern for organisations. As part of a comprehensive cyber security strategy, our service offers tailored cyber incident tabletop exercises.

These exercises, available both on-site and remotely, guide you through realistic incident scenarios. By simulating these situations we rigorously test an organisation's crisis management capabilities, evaluates incident readiness, and pinpoints areas for improvement in response strategies.

What's involved?

PTP walks you through a series of cyber incident scenarios to test your crisis skills and cyber incident response readiness.

Scenarios are customised to the context and environment in which the organisation operates, you may choose to focus on specific threats that are of greatest concern for your business.

Different types of exercises are offered depending on the people who need to be involved:

- **Gold Team** exercises focus on strategic decision makers
- **Silver Team** exercises are for tactical personnel such as heads of department and team leaders
- **Bronze Team** exercises are targeted at operational employees such as technical incident responders and IT professionals.

What is included?

PTP has a wealth of experience in delivering digital forensics and incident response services.

Tailored scenarios

The tabletop exercises are meticulously customised to match the specific context and environment of each client's business.

This ensures that the challenges presented during the exercise are directly relevant to their industry, business model, and unique cyber threat landscape.

Emulating real incidents

The exercises consist of several "injects" designed to emulate the fluidity of a genuine cyber incident.

These injects challenge teams to think on their feet, adapt to evolving situations, and make critical decisions.

What are the benefits?

Realistic Preparedness: Almost every organisation will encounter a cyber incident. Preparedness is no longer optional; it is a necessity. These exercises create a safe and controlled environment for team members to practice response procedures, collaboration, and decision-making skills. Regular exercises ensure that when an incident occurs, the organisation can respond swiftly and effectively while minimising impact.

Tailoring to Objectives: Each organisation has unique goals. The exercises can be fully customised to meet specific objectives, whether testing a newly developed incident response plan, enhancing team collaboration, or assessing the effectiveness of existing strategies. PTP collaborates closely with you to ensure the exercises align with your expectations and objectives.

PEN TEST PARTNERS

Why buy a Tabletop Exercise?

It is likely that all businesses will experience a cyber incident at some point. PTP has a wealth of experience in delivering digital forensics and incident response services. Simulations are bespoke and suit the organisation's objectives, requirements, and operational context. Regularly testing processes and procedures is vital for incident response readiness

Testing cyber incident responses processes and procedures may be a requirement for achieving and maintaining industry certifications, and may even be a regulatory requirement for businesses in some industries. PTP offers additional services that complement the tabletop exercises, these include incident response policy and playbook development as well as Digital Forensics and Incident Response Maturity Reviews.

Problems it solves

- Organisations that practice and prepare with simulations are more likely to operate effectively during a real cyber incident.
- Prevents incident response related processes, procedures, and knowledge from going stale.
- Incident response exercises are often a requirement for several formal certifications and regulations.
- Helps organisations address opportunities for improvement before incidents occur.
- Improves confidence with stakeholders including clients, partners, and regulators.

CREST

PEN TEST

STAR
Intelligence-led PT

STAR-FS
Intelligence-led PT

CSIR

OVS

CBEST

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

ASSURE

CYBER ESSENTIALS

bsi. ISO/IEC 27001 Information Security Management

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

PTP Services

Testing

- Penetration Testing – CHECK, CREST
- CREST STAR & CBEST
- Red Teaming
- Application Testing
- Infrastructure testing
- Mobile App & Device Testing
- Application Code Reviews
- Cloud Testing
- Social Engineering
- API & Web Services testing

Training

- Security Awareness Training
- Phishing Simulation & Training
- Hardware Hacking Workshops
- Developer Coding Training

PTP Tools

- PAPA Password Auditing Service

DFIR

- Digital Forensics
- Incident Response
- Mobile Device Forensics
- Incident Response Retainer
- Compromise Assessment

Specialist testing

- Maritime Cyber Security
- Rail Cyber Security
- Automotive
- Aviation & Aerospace
- IoT Security Testing
- ICS / OT / IIoT
- GBEST & TBEST

Consultancy

- PCI QSA
- ISO27001
- Virtual CISO
- General Security Consultancy
- Policy Creation and review

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

PEN TEST PARTNERS

Contact us today:
info@pentestpartners.com
+44 (0)20 3095 0500

3rd Party Supplier Assurance

Why do clients need this?

Breaches originating from the supply chain are becoming more common. Supply chains present large and complex attack vectors.

PTP supports clients in assuring their third parties and suppliers. It reduces the risk of data breach and loss of availability, it supports BAU, and bolsters user and client confidence.

This service offers clients a sliding scale of support from self-assessment led reviews, to fully audited engagements, based on the specific level of assurance that you want.

What's involved?

An independent review of your third party suppliers to identify the potential risks they present to you.

It ensures that information security and data privacy requirements are accounted for in the vendor selection process.

We can deliver this as a one-off service, or an ongoing engagement, where regular supplier reviews are needed.

Three different service levels are available, depending on the compliance boxes that you need to tick.

How does it work?

PTP evaluates client's existing suppliers using market research, referrals, reputation, financial stability, experience, and references.

PTP then conducts risk assessments using data security, financial and operational risk.

Depending on the findings PTP may provide questionnaires or conduct audits to provide evidence and documentation relating to supplier certifications, processes, and policies.

These will be based on controls from standards such as ISO 27001:2022 Annex A and the Cloud Security Alliance Cloud Control Matrix (CSA CCM).

Where necessary PTP will oversee contractual negotiations to discuss SLAs, data protection clauses, and other essential elements.

Problems solved

Reduces risk from third-party supply chains.

Frees up internal resource while providing a consistent approach.

Can be used as a training activity for your teams to develop their assurance capability.
Ensures that clients fulfil contractual requirements relating to the third-party supply chain.

Prerequisites

It's beneficial if clients have a specific standard or framework in mind.
It's not 100% necessary though as PTP can help clients work out the standards that will be best.

PTP will need dedicated personnel to work with us.

PTP needs clients to be available to join us in meaningful discussions with third party suppliers.

PEN TEST PARTNERS

Annual 3rd party supplier assurance - 3 stages

Low Risk

- Self-assessment sent to 3rd party
- PTP reviews responses and provides risk feedback
- If medium or high risks are identified PTP progresses to the next higher level review
- Reporting provided listing our recommendations

Medium Risk

Low risk plus:

- Interviews conducted with 3rd parties to review and validate responses
- If high risks are identified PTP progresses to the high risk review
- Reporting provided listing our recommendations

High Risk

Medium risk plus:

- Full sampling review conducted, remotely or onsite, as required
- Independent evidence of control effectiveness
- Reporting provided listing our recommendations

CREST

PEN TEST

STAR
Intelligence-led PT

STAR-FS
Intelligence-led PT

CSIR

OVS

CBEST

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

ASSURE

CYBER ESSENTIALS

bsi. ISO/IEC 27001 Information Security Management

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

PTP Services

Testing

- Penetration Testing – CHECK, CREST
- CREST STAR & CBEST
- Red Teaming
- Application Testing
- Infrastructure testing
- Mobile App & Device Testing
- Application Code Reviews
- Cloud Testing
- Social Engineering
- API & Web Services testing

Training

- Security Awareness Training
- Phishing Simulation & Training
- Hardware Hacking Workshops
- Developer Coding Training

PTP Tools

- PAPA Password Auditing Service

DFIR

- Digital Forensics
- Incident Response
- Mobile Device Forensics
- Incident Response Retainer
- Compromise Assessment

Specialist testing

- Maritime Cyber Security
- Rail Cyber Security
- Automotive
- Aviation & Aerospace
- IoT Security Testing
- ICS / OT / IIoT
- GBEST & TBEST

Consultancy

- PCI QSA
- ISO27001
- Virtual CISO
- General Security Consultancy
- Policy Creation and review

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

PEN TEST PARTNERS

Contact us today:
info@pentestpartners.com
+44 (0)20 3095 0500

3rd Party Vendor Selection

Why do clients need this?

This service guides clients through the procurement process. Selecting the wrong vendor or supplier can result in long lasting consequences. Supply chain attacks are becoming more common, and more sophisticated. PTP can help clients make informed supplier decisions with a view to safeguarding sensitive data and maintaining compliance.

As well as this PTP will provide comprehensive advice and assistance for creating essential documentation, based on sensible criteria developed from standardised sets of information security and data privacy requirements.

What's involved?

PTP helps clients select third-party suppliers and vendors.

This is particularly useful for identifying third parties such as managed service providers, managed security service providers, and software as a service vendors.

PTP can also help with the tender process by advising on how to create essential documentation such as RFP's and contracts.

To enable all this, PTP has developed criteria based on a standardised sets of information security and data privacy requirements.

How does it work?

PTP run requirement gathering and process analysis sessions to establish precisely what the client needs from a vendor.

Initial fact-finding interviews will be conducted with suppliers to match client criteria to at least three shortlisted suppliers.

Prerequisites

It's beneficial if clients have a specific standard or framework in mind. It's not 100% necessary as PTP can work with clients to identify what will be most beneficial for clients.

PTP will need dedicated personnel for the duration of the engagement.

PTP need clients to be able to engage in meaningful discussions and potential third-party suppliers during the engagement.

Problems solved

Vendor selection and tender processes can be extremely process intensive, especially if specific technical knowledge is required to ensure the correct vendor/product is selected.

There may be contractual and regulatory obligations pertaining to supplier assurance.

This may be a requirement for formal certification.

It may be more cost effective to engage with PTP to complement clients' existing staff, rather than hiring a full-time resource.

Conflict of interest promise

If it arises, PTP will tell you when any preferred suppliers are suggested by clients or appear on a shortlist.

PTP will include suitable alternatives for balance.

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, 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.