CYBERSECURITY SERVICES REGULATION OFFICE

BUYER'S GUIDE FOR PENETRATION TESTING SERVICE

"Discover your cybersecurity weaknesses before the bad guy does"

1. What is PT?

Penetration Testing ("PT") is the act of simulating attacks to test the cybersecurity of infocomm technology, operational technology, industrial control systems, infrastructure, network or web/ mobile applications and perimeter defences (collectively "systems").

2. Why do you need PT?

With the proliferation of digitalisation, **organisations are increasingly exposed to cyber threats and attacks which can adversely impact your business in several ways:**

- Your business will suffer loss of reputation, revenue and the goodwill of your customers and stakeholders.
- Your business may breach the law if confidential and sensitive data and customer information is leaked.

Engaging a good licensed PT service provider can help you reduce the chance of a successful cyber-attack by simulating attacks to discover your cybersecurity weaknesses and recommend ways to strengthen your cybersecurity posture.

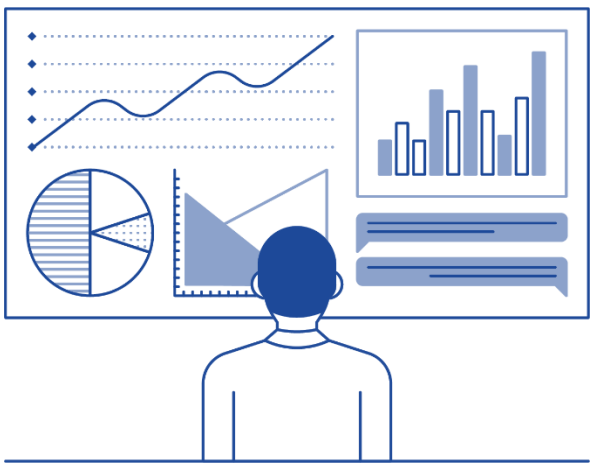
3. When to do PT?

A common practice is to do PT during pre- and post-deployment of a new systems or any part of it, or following any major changes to the systems.

It is advisable to conduct regular PT as the threat environment is constantly evolving and new vulnerabilities may become exploitable by attackers. Conduct regular PT at a frequency that commensurate with the criticality of your organisation's assets, the consequences if attacked, and the available budget.

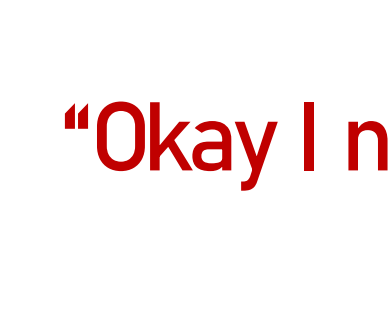
Disclaimer: This guide is produced by the Cybersecurity Services Regulation Office as an introductory guide for buyers of PT services. Buyers are advised to do their due diligence when selecting a licensed PT service provider and to consult relevant references to ensure that their requirements are met.

“Okay I need PT, what should I do next?”



START by reviewing your target environment

Know your target environment, your risk appetite, and the impact of an attack to your business needs and obligations.



DEFINE the objective & scope of PT

Understand the purpose and scope of PT, deliverables, timeline, and time horizon.

DETERMINE the style and type of PT you need

Do you require black, white, or grey box PT (i.e. provision of system’s information to, and granting access to computer systems for the licensed PT service provider)?

EVALUATE the available options

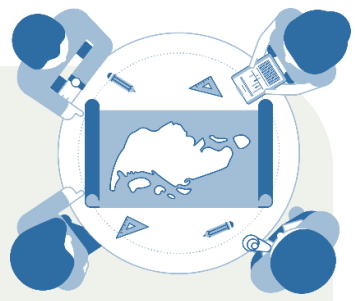
Based on the information gathered, assess the available options, and form a project team.

CONSULT a licensed PT service provider if you require assistance

A good PT service provider can walk you through the process and provide you with guidance to properly scope the PT. Obtain proposals from a few licensed PT service providers before deciding.

Disclaimer: This guide is produced by the Cybersecurity Services Regulation Office as an introductory guide for buyers of PT services. Buyers are advised to do their due diligence when selecting a licensed PT service provider and to consult relevant references to ensure that their requirements are met.

"Execution is key and prompt implementation of remediation action is crucial"

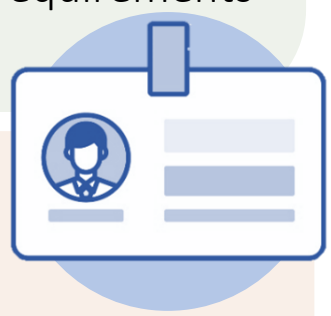


4. What happens during PT and what to expect from a licensed PT service provider?

The following is a typical workflow when working with a licensed PT service provider:

- Start with planning and preparation. This includes working together to define the PT scope and establish the methods of testing.
- Next, the licensed PT service provider will conduct research, analysis and vulnerabilities scanning to gather information and vulnerabilities that can be exploited.
- This is followed by the actual execution of PT activities.
- Lastly, obtain a comprehensive report from the licensed PT service provider that includes high-level management style reporting and technical details on vulnerabilities discovered and recommendations for remediation.

After the PT, promptly remediate weaknesses discovered to strengthen your cybersecurity posture, policies, and processes. Conduct a follow-up test to ensure that weaknesses are eradicated. Devise a plan to conduct regular PT based on your organisation's requirements and risk appetite.



5. How to select a licensed PT service provider?

Review the credentials and qualifications of licensed PT service provider and team members.

- Check whether the PT service provider is licensed.
  Tips: *CSRO website (QR code on right) provides a list of licensed PT service provider.*
- What is the company's reputation and credibility e.g. is the company CREST*accredited?
- Do the team members have relevant experiences, qualifications, and professional certifications e.g. GIAC Exploit Researcher and Advanced Penetration Tester (GXPN), Offensive Security Certified Professional (OSCP) or CREST PT related certifications?
- What projects have they done in the past? Request for testimonials or references from clients and sample reports to compare the quality and comprehensiveness between different licensed PT service providers.

Understand your licensed PT service provider's liability coverage and insurance as you are legally allowing the licensed PT service provider to hack your systems and there is a risk that things may go wrong e.g. loss of customer or propriety data, or compromised systems taking longer than expected to restore its normal function or incurring additional cost to be fixed.

**CREST is an international not-for-profit accreditation and certification body that represents and supports the technical information security market. The CREST Singapore chapter, launched in 2016 in partnership with CSA and the Association of Information Security Professionals (AISP), provides CREST certifications to ensure that PT service providers and professionals are trustworthy, competent, and equipped with the necessary technical skills. Check out CREST website for accredited companies providing PT services and CREST Guide to Penetration Testing.*

Disclaimer: This guide is produced by the Cybersecurity Services Regulation Office as an introductory guide for buyers of PT services. Buyers are advised to do their due diligence when selecting a licensed PT service provider and to consult relevant references to ensure that their requirements are met.