CREST

A Guide to Penetration Testing

December 2022

Published by:

CREST
Tel: 0845 686 5542
admin@crest-approved.org
www.crest-approved.org

Principal Author

Jason Creasey,
Managing Director, Jerakano Limited

Principal reviewer

Ian Glover,
President, CREST

DTP notes

For ease of reference, the following devices have been used throughout this Penetration Testing Guide.

Acknowledgements

CREST would like to extend its special thanks to those CREST member organisations which took part in interviews and to those clients who agreed to be featured in case studies.

Warning

This Guide has been produced with care and to the best of our ability. However, CREST accepts no responsibility for any problems or incidents arising from its use.

💡 A good tip

🔔 A timely warning

📖 An insightful project finding

Contents

Part 1 – Introduction and overview

Part 2 – Understanding the key concepts

Part 3 – Preparation

Part 4 – Testing

Part 5 – Follow up

Part 6 – Penetration testing programme maturity assessment

Part 7 – Conclusions

Part 1 – Introduction and overview

About this Guide

This *Penetration Testing Guide* (the Guide) provides practical advice on the establishment and management of a penetration testing programme, helping you conduct effective, value-for-money penetration testing as part of a technical security assurance framework. It is designed to enable your organisation to prepare for penetration tests, conduct actual tests in a consistent, competent manner and follow up tests effectively.

The Guide presents a useful overview of key concepts you need to understand to conduct well-managed penetration tests. It explains what a penetration test is (and is not) and outlines the test's strengths and limitations. The guide describes why an organisation would choose an external penetration testing services provider to help it plan for, and undertake, tests effectively, ensuring that vulnerabilities are identified and remediated.

Presented as a useful three stage approach, as shown in Figure 2 on page 11, the Guide then provides guidance on how to take the required actions to:

1. Prepare for penetration testing

- As part of a technical security assurance framework
- Managed by an appropriate penetration testing governance structure
- Considering the drivers for testing
- The purpose of testing and target environments, and
- Appointing suitable suppliers to perform tests

2. Conduct penetration tests enterprise-wide

- Approving testing style and type
- Allowing for testing constraints
- Managing the testing process
- Planning for and carrying out tests effectively
- Identifying, investigating and remediating vulnerabilities

3. Carry out appropriate follow up activities

- Remediating weaknesses
- Maintaining an improvement plan, and
- Delivering an agreed action plan

All aspects of a penetration testing programme (which includes determining requirements, performing the actual tests and carrying out follow up activities) need to be well managed. For example, by establishing an assurance process to oversee testing, monitoring performance against requirements and ensuring appropriate actions are being taken.

The purpose of this Penetration Testing Guide is to help you:

- Understand objectives for conducting a penetration test
- Gain an overview of the key components of an effective penetration testing approach
- Develop an appropriate penetration testing programme
- Identify what needs to be considered when planning for and managing penetration tests
- Learn about the penetration testing process – and associated methodologies
- Determine criteria upon which to base selection of appropriate service providers

Scope

This Guide focuses on helping your organisation undertake effective penetration testing enterprise-wide, at the right time and for the right reasons. It is designed to help organisations which procure penetration services from external suppliers, but will also be useful for organisations conducting penetration tests themselves.

There are often special requirements for penetration testing service providers. For example, when supplying services to UK Government departments, the organisations supplying services must have CHECK 'green light' clearance from the National Cyber Security Centre (NCSC). Although these specific requirements are out of scope for this guide, they are typically covered by the contents of this Guide anyway. Further information on CHECK can be found at: **www.ncsc.gov.uk/articles/using-check-provider**

To carry out penetration testing effectively you will need to build an appropriate penetration testing programme. The programme's maturity can be assessed against a suitable maturity model by using the CREST suite of penetration testing maturity assessment tools (see **Part 6** – Penetration testing programme maturity assessment for more details).

The penetration testing maturity assessment tools form part of a series of assessment tools developed by CREST, including high level and detailed Cyber Security Incident Response Maturity Assessment Tools.

Rationale

Many organisations are extremely concerned about potential and actual cyber security attacks, both on their own organisation and in ones similar. Many of these attacks exploit weaknesses in an organisation's applications and underlying infrastructure. To help identify as many of these vulnerabilities as possible within a critical timescale – and address them effectively – many carry out penetration testing. However, establishing and managing a suitable penetration testing programme enterprise-wide can be a very difficult task, even for the most advanced organisations.

Much of the material in this guide is based on the findings of a research project – conducted by Jerakano Limited on behalf of CREST – about the main requirements organisations have for considering and conducting penetration tests. One of the main reasons for commissioning a research project was that CREST member's clients were often unclear about how best to procure penetration testing services.

A summary of CREST activities can be found at: **www.crest-approved.org**. Where relevant, CREST benefits are also highlighted throughout the Guide.

The research project was based on:

- Reviews of relevant material produced by industry bodies, including CPNI, OWASP, OSSTM and PTES (see tip below)
- Desktop (mainly web-based) research
- Technical workshops attended by experienced penetration testing experts, as well as representatives from relevant government and industry bodies
- Analysis of questionnaire responses regarding procurement of penetration testing services
- Interviews with leading suppliers of penetration testing services
- Case studies of major client organisations

Some of the principle sources of material reviewed included:

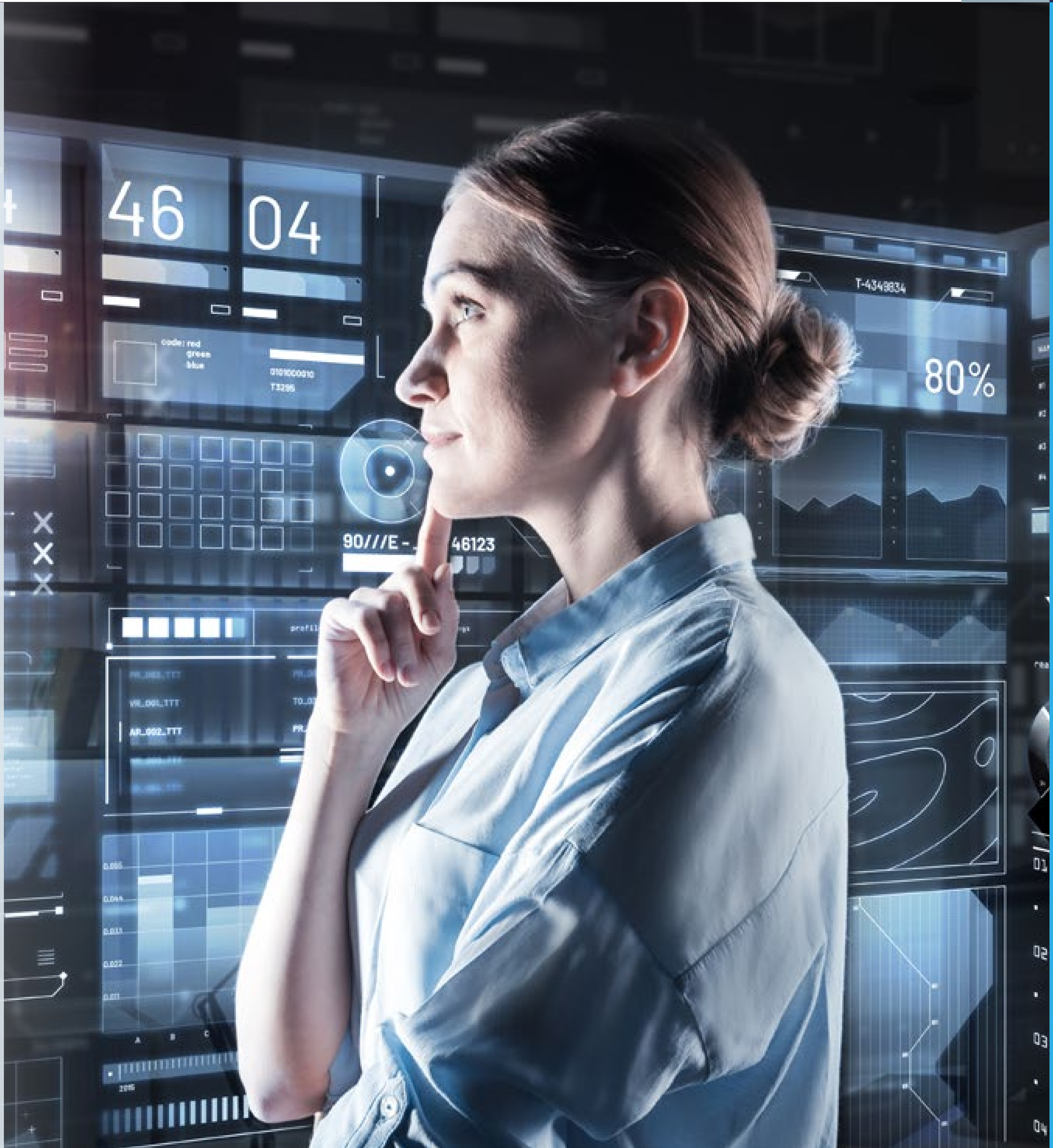
- The ***Open Source Security Testing Methodology Manual (OSSTMM)*** from The Institute for Security and Open Methodologies (ISECOM)
- The ***Open Web Application Security Project® (OWASP)*** from OWASP foundation
- The ***Penetration Testing Execution Standard (PTES)***, produced by a group of information security practitioners from all areas of the industry
- The ***Best Practice Guide*** – Commercially available penetration testing from the Centre for the Protection of National Infrastructure (CPNI)

Audience

Historically, mainly due to legal or regulatory requirements, many organisations requiring penetration tests have come from government departments. These include utilities (e.g. gas, water or telecoms); pharmaceuticals, banks and other financial institutions.

However, an increasing array of organisations now conduct penetration testing, not just for compliance reasons, but because of the online nature of nearly all businesses today and the increasing threat from real (often cyber) attacks. Consequently, this guide is designed for all market sectors.

The guide's main intended audience is those involved in the management of a penetration testing programme (including procurement of penetration testing services), such as IT, project or security managers.



Part 2 – Understanding the key concepts

Introduction

Organisations like yours have the evolving task of securing complex IT environments while delivering business and brand objectives. The threat to key systems is ever increasing and the probability of a security weakness being accidentally exposed or maliciously exploited needs to be continually assessed – such as via a penetration test – to ensure that level of risk is acceptable to the business.

A penetration test ('pen test') involves a variety of manual and automated techniques to simulate an attack on an organisation's information security arrangements – either from malicious outsiders or your own staff.

Undertaking a series of penetration tests will help test your security arrangements and identify improvements. When carried out and reported properly, a penetration test can give you knowledge of nearly all technical security weaknesses and provide the information and support required to remove or reduce those vulnerabilities.

Research shows there are also other significant benefits derived from effective penetration testing, which can include:

- A reduction in ICT costs over the long term
- Improvements in the technical environment, reducing support calls
- Greater levels of confidence in the security of your IT environments
- Increased awareness of the need for appropriate technical controls

Many companies choose to appoint a trusted, specialist organisation (a CREST member), employing qualified professionals (such as CREST-qualified staff), to help conduct penetration tests. Although these suppliers are sometimes employed just to conduct testing, they can also help when specifying requirements, defining the scope of the test and developing a management framework.

Penetration testing is not, however, a straightforward process – nor is it a remedy for all ills. It is often very technical in nature, with methods and outputs often riddled with jargon, which can be daunting for organisations considering the need for this sort of complex testing. Organisations report several difficulties when conducting penetration tests, which include:

- Determining the depth and breadth of coverage of the test
- Identifying what type of penetration test is required
- Managing risks associated with potential system failure and exposure of sensitive data
- Agreeing the targets and frequency of tests
- Assuming that by fixing vulnerabilities uncovered during a penetration test their systems will then be 'secure'

There are many buzzwords that can be associated with penetration testing (rightly and wrongly) including ethical hacking, tiger teaming, vulnerability analysis, security testing, assessment or assurance.

When considering the need for penetration testing, organisations may ask:

- What exactly is a penetration test, and how does is it differ to other types of security techniques?
- What are the compelling reasons to perform a penetration test?
- Who should conduct the test?
- How do we go about it?
- What are the risks and constraints we should be concerned about?
- How do we decide which supplier to choose?

This part of the guide presents answers to these questions, while the remainder explores responses in more detail.

Definition of a penetration test

Penetration testing involves manual and automated techniques to simulate an attack on an organisation's information security arrangements. It should be conducted by a qualified and independent penetration testing expert, sometimes referred to as an ethical security tester. Penetration testing looks to exploit known vulnerabilities but should also use the tester's expertise to identify specific weaknesses – unknown vulnerabilities – in an organisation's security arrangements.

The penetration testing process involves:

- Active analysis of the system for potential vulnerabilities that could result from poor or improper system configuration
- Known and unknown hardware or software flaws, and
- Operational weaknesses in process or technical countermeasures

This analysis is typically carried out from a potential attacker's perspective, and can involve active exploitation of security vulnerabilities.

A Penetration Test is typically an assessment of IT infrastructure, networks and business applications to identify attack vectors, vulnerabilities and control weaknesses. The two most common forms of penetration testing are:

- ***Application*** penetration testing (typically web applications), which finds technical vulnerabilities
- ***Infrastructure penetration testing***, which examines servers, firewalls and other hardware for security vulnerabilities

Other forms of penetration testing include:

- Mobile application penetration testing
- Client server (or legacy) application penetration testing
- Device penetration testing, (including workstations, laptops and consumer devices (eg. tablets and smartphones)
- Wireless penetration testing
- Telephony or VoIP penetration testing

The penetration testing process typically includes:

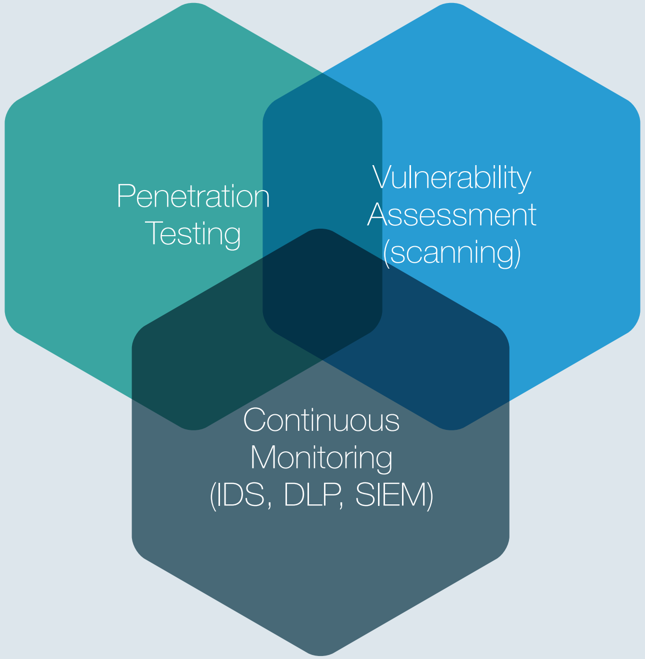
- Conducting research
- Identifying vulnerabilities
- Exploiting weaknesses
- Reporting findings, and
- Remediating issues

Each step is explored in ***Part 4 – Conducting penetration tests***.

Technical security testing

Penetration testing is well established and one of a range of ways for testing the technical security of a system. However, it can easily be confused with other forms of technical security testing, particularly Vulnerability Assessment. In some cases, there can also be a relationship with continuous monitoring services. These include Intrusion detection or prevention systems (IDS), Data Loss Prevention (DLP) technology or processes and Security information and event management (SIEM). How these technical security services overlap is shown in Figure 1 right.

Figure 1: Technical security weakness discovery techniques


Penetration Testing
Vulnerability Assessment (scanning)
Continuous Monitoring (IDS, DLP, SIEM)

Vulnerability Assessments

Vulnerability assessment (sometimes referred to as 'scanning') is the use of automated tools to identify known common vulnerabilities in a system's configuration. Vulnerability Assessment tools scan the information systems environment to establish whether security settings have been switched on and consistently applied – and that appropriate security patches have been deployed.

Vulnerability assessment typically seeks to validate the minimum level of security that should be applied – and is often the pre-cursor to more specialised penetration testing. It does not exploit vulnerabilities identified to replicate a real attack, nor does it consider overall security management processes and procedures that support the system.

A penetration test is an ethical attack simulation intended to demonstrate or validate the effectiveness of security controls in a particular environment by highlighting risks posed by actual exploitable vulnerabilities. It is built around a manual testing process, which is intended to go much further than the generic responses, false positive findings and lack of depth provided by automated application assessment tools (such as those used in a vulnerability assessment).

Penetration testing in context

Penetration testing should be considered in the context of security management as a whole. To gain an appropriate level of assurance, reviews should be conducted. These reviews are often aligned to standards such as ISO 27001, COBIT 2019 or the ISF Standard of Good Practice.

ISO / IEC 27001 is an international standard on how to manage information security.
www.iso.org/isoiec-27001-information-security.html

COBIT (Control Objectives for Information and Related Technologies) is a framework created by ISACA for information technology (IT) management and IT governance. COBIT 2019 is a framework for the governance and management of enterprise information and technology (I&T) that supports enterprise goal achievement.
www.isaca.org/resources/cobit

The Standard of Good Practice for Information Security, published by the Information Security Forum (ISF), is a business-focused, practical and comprehensive guide to identifying and managing information security risks in organisations and their supply chains.
www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-information-security-2020/

While these standards reference penetration testing, they do so mainly from a management perspective. Most security management standards do not describe penetration testing in any depth, nor put testing strategies into context. So, systems and environments that comply with these standards may not actually be technically secure. A balanced approach of technical and non-technical testing must be taken to ensure the overall integrity of security controls.

There are many forms of testing – ideally performed by an independent (often external) team – that help provide appropriate levels of information security assurance. These include technical reviews of applications development and implementation standards, security reviews of the Information Security Management System (ISMS) and compliance audits.

While other forms of security assurance provide only a theoretical description of vulnerability, penetration testing demonstrates actual vulnerability against defined and real threats. Penetration test results can be more compelling and demonstrable to both senior management and technical staff.

Assurance cannot be gained from any one of these activities in isolation – penetration testing has a key role to play. It is important to consider how testing is built into the system's development lifecycle activities. Remember regular testing can provide an industry benchmark against which improvements in the technical security environment can be measured.

"Organisations should not describe themselves as secure – there are only varying degrees of insecurity"

Penetration testing limitations

Undertaking a series of penetration tests will help test some of your security arrangements and identify improvements, but it is not fool proof. For example, a penetration test:

- Covers just the target application, infrastructure or environment selected
- Focuses on exposures in technical infrastructure. It is not intended to cover all the ways critical or sensitive information can leak out of your organisation
- Plays only a small part (despite often including social engineering tests) in reviewing the people element (often the most important element of an organisation's defence system)
- Is only a snapshot of a system at a point in time
- Can be limited by legal or commercial considerations, limiting the breadth or depth of a test
- May not uncover all security weaknesses – for example, due to restricted scope or inadequate testing
- Provides results that are often technical in nature and need to be interpreted in a business context

Penetration tests need to supplement a full range of security management activities, including those laid out in ISO 27001, COBIT 2019 or the ISF Standard of Good Practice.

Penetration testing challenges

In addition to penetration testing limitations, many organisations are facing a number of more general challenges when carrying out penetration testing.

Findings from the research project indicated the top six penetration testing challenges for organisations included difficulties in:

1. Determining the depth and breadth of coverage of the test
2. Identifying what type of penetration test is required
3. Understanding the difference between vulnerability scanning and penetration testing
4. Identifying risks associated with potential system failure and exposure of sensitive data
5. Agreeing targets and frequency of tests
6. Assuming that by fixing vulnerabilities uncovered during a penetration test systems will then be 'secure'

Other challenges highlighted included difficulties in:

- Establishing a business case for a test to be undertaken
- Understanding the costs of external services – and determining the true overall cost
- Remediating system vulnerabilities effectively
- Finding a suitable penetration testing expert when required (e.g. at short notice)

For these challenges to be identified and addressed effectively, an organisation should adopt a systematic, structured approach to penetration testing as part of a wider penetration testing programme, including selection and management of external suppliers.

Using external suppliers

Organisations can carry out penetration testing themselves, sometimes very successfully. More often, they decide to use specialist third-party penetration testing providers.

There are many reasons why, such as helping meet the challenges outlined in the previous section.

Findings from the research project indicated that the top three reasons (by some way) why organisations hire external suppliers are because these suppliers can:

1. Provide more experienced, dedicated technical staff who understand how to carry out penetration tests effectively
2. Perform an independent assessment of their security arrangements
3. Carry out a full range of testing (e.g. black, white or grey box, internal or external, infrastructure or web application, source code review and social engineering)

Other reasons given for using external suppliers are because they can:

- Deploy a structured process and plan, developed by experts
- Increase scope and frequency of tests
- Conduct short term engagements, eliminating the need to employ your own specialised (and often expensive) staff – and reducing training (and re-training) costs of internal teams
- Take advantage of automation (e.g. penetration testing workflows, or importing vulnerability management reports)

There are many benefits in procuring penetration testing services from a trusted, certified external company which employs professional, ethical and highly technically competent individuals. CREST member companies are certified penetration testing organisations that fully meet these requirements, having been awarded the gold standard in penetration testing, building trusted relationships with their clients.

> **“What we are looking for from a supplier is certainty, prioritisation, trust and security”**

The need for a penetration testing programme

The main drivers for penetration testing include a high degree of concern about:

- A growing requirement for compliance
- The impact of serious (often cyber-related) security attacks on similar organisations
- Use of a greater number and variety of outsourced services
- Significant changes to business processes
- Raising awareness of possible cyber security attacks

However, establishing and managing a suitable penetration testing programme can be a difficult task, even for the most advanced organisations.

When performing penetration tests, some adopt an ad hoc or piecemeal approach, often depending on the needs of a particular region, business unit – or the IT department. While this approach can meet some specific requirements, it is unlikely to provide real assurance about the security condition of your enterprise-wide systems.

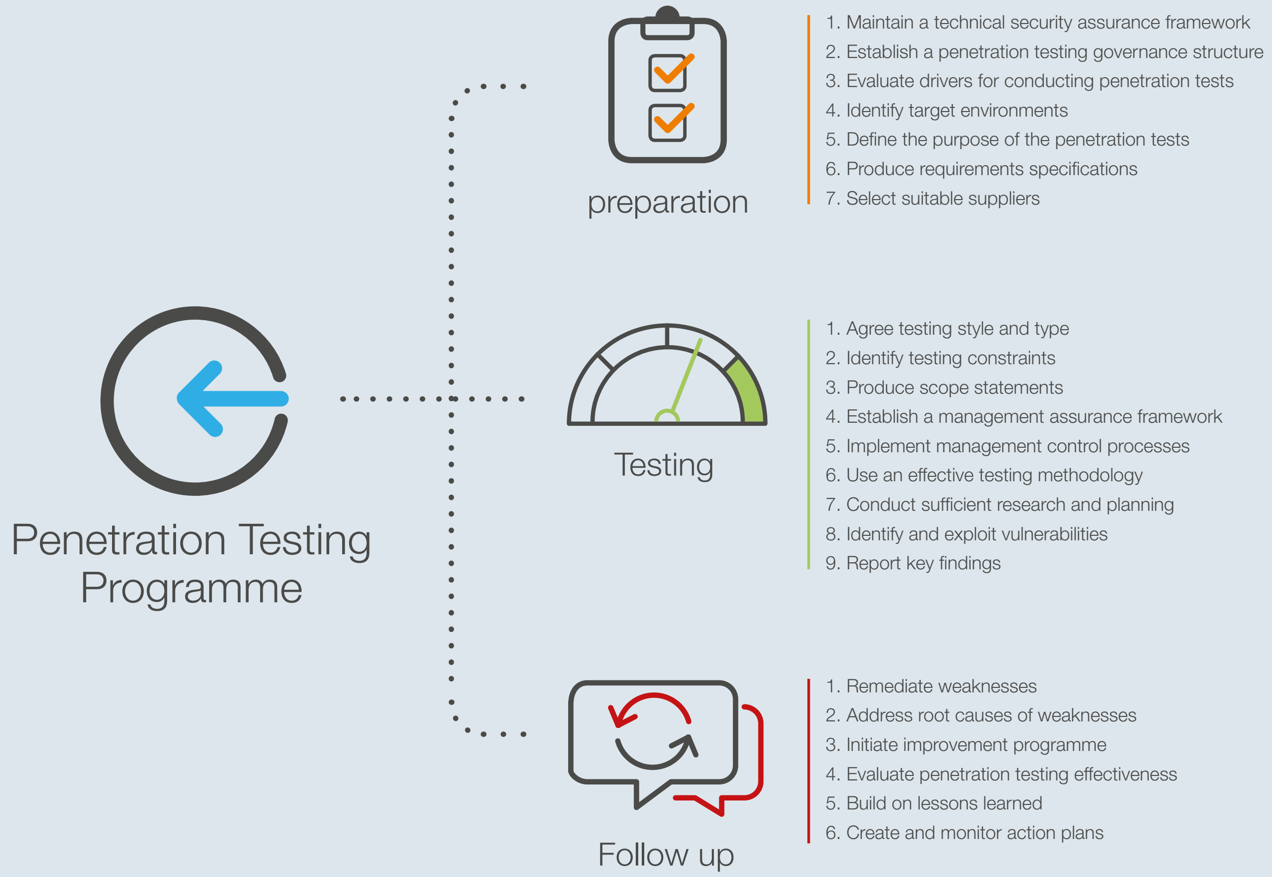
It is often more effective to adopt a more systematic, structured approach to penetration testing as part of an overall testing programme, ensuring that:

- Business requirements are met
- Major system vulnerabilities are identified and addressed quickly and effectively
- Risks are kept within acceptable business parameters

Outline of a penetration testing programme

Your penetration testing programme should cover key activities required to prepare for penetration testing. Any programme must include an appropriate set of tests, delivered in a consistent, well-managed way and measures to ensure the tests are followed up effectively. The CREST approach comprises three main stages, supported by 22 detailed steps, as outlined in Figure 2 below.

Figure 2: The Penetration Testing Programme



1. Maintain a technical security assurance framework
2. Establish a penetration testing governance structure
3. Evaluate drivers for conducting penetration tests
4. Identify target environments
5. Define the purpose of the penetration tests
6. Produce requirements specifications
7. Select suitable suppliers

1. Agree testing style and type
2. Identify testing constraints
3. Produce scope statements
4. Establish a management assurance framework
5. Implement management control processes
6. Use an effective testing methodology
7. Conduct sufficient research and planning
8. Identify and exploit vulnerabilities
9. Report key findings

1. Remediate weaknesses
2. Address root causes of weaknesses
3. Initiate improvement programme
4. Evaluate penetration testing effectiveness
5. Build on lessons learned
6. Create and monitor action plans

Your penetration testing programme must include appropriately skilled people, guided by well-designed, repeatable processes and effective use of relevant technologies. This will enable you to conduct thorough penetration tests, successfully identifying and addressing vulnerabilities – and to prevent new ones from occurring.

The maturity and effectiveness of your penetration testing programme should be evaluated regularly against approved criteria to help determine if objectives were met and value for money obtained from supplier(s).

Positioning the penetration testing programme

The penetration testing programme should be part of – or at least aligned with – an approved technical security assurance framework, focused on protecting your most critical information and systems.

You should not consider undertaking any significant penetration testing unless your organisation has already implemented a range of basic security controls (also referred to as cyber security hygiene), such as malware protection, firewalling, system / network patching and vulnerability assessments.

A primary objective of the UK government's National Cyber Security Strategy – a useful benchmark – is to make the UK a safer place to conduct business online. CREST was engaged by the National Cyber Security Centre (NCSC), (the information security arm of the UK government), to develop an assessment framework to support the government's "Cyber Essentials" scheme, which forms a key deliverable of this strategy.

The Cyber Essentials scheme's five critical controls cover boundary firewalls and internet gateways, secure configuration, access control, malware protection and patch management. The scheme is applicable to all organisations, giving basic protection from the most prevalent forms of cyber threat.

The scheme's technical controls, selected by industry experts, reflect those covered in well-established standards, as mentioned earlier.

The Assurance Framework, leading to the award of Cyber Essentials and Cyber Essentials Plus certificates, is designed to be light-touch and achievable at low cost. The two certificates give a choice over the level of assurance desired, but the Cyber Essentials Plus option is recommended as it includes external testing of an organisation's cyber security approach.

Cyber Essentials offers a sound foundation of basic hygiene measures that all types of organisations can implement and potentially build upon. Cyber Essentials defines a set of controls which, when properly implemented, will provide organisations with basic protection from the most prevalent forms of cyber threats coming from the Internet. In particular, it focuses on those threats which require low levels of attacker skill, and which are widely available online.

The UK government believes that implementing these measures can significantly reduce an organisation's vulnerability. However, it does not offer a 'silver bullet' to remove all cyber security risk.; For example, it is not designed to address more advanced, targeted attacks. and hence organisation. Those facing such threats will need to implement additional measures as part of their security strategy, such as penetration testing.

Red and Blue Teaming

Many security assessments focus on breadth, rather than depth, and are constrained to the given component being tested. A Red Team is an internal or external group that plays the role of an enemy or competitor, and provides security feedback from that perspective. Red teams are used in many fields, especially in cybersecurity, airport security, the military, and intelligence agencies. ‘Red Teaming’ gives organisations a more realistic, real-world view into what an attacker might, and can, do to gain access to your assets. The practice is similar, but not identical to, penetration testing, and involves pursuit of one or more objectives.

A ‘Red Teamer’ will not solely focus on just your network infrastructure or web applications. Instead they will identify potential weak points and string together seemingly unrelated vulnerabilities to create composite attack scenarios, as realistically as such an attack would play out in real life.

There are a number of approaches to Red Teaming, supported by various definitions, many of which can be found in British and American defence publications. For example, the MOD Red Teaming Guide, Third Edition, October 2021 defines a red team as:

> **‘A team that is formed with the objective of subjecting an organisation’s plans, programmes, ideas and assumptions to rigorous analysis and challenge’.**

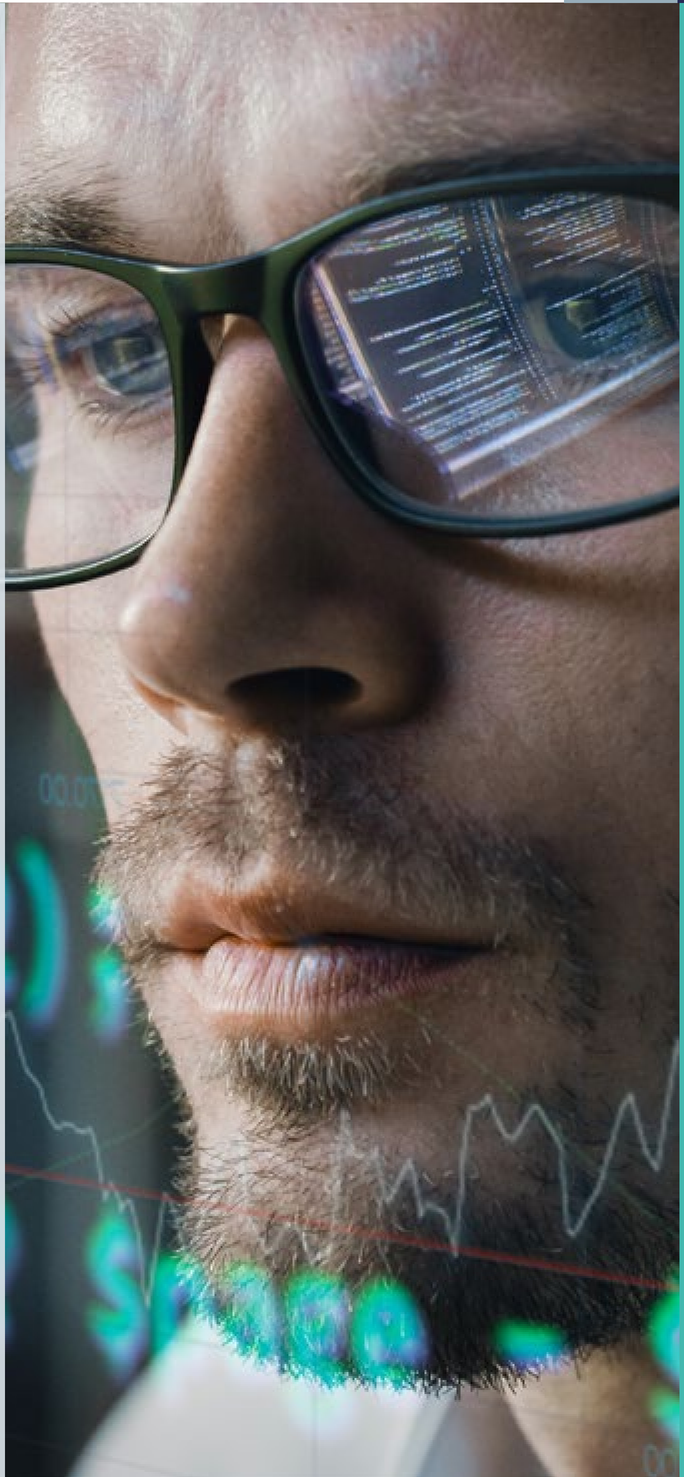
Organisations establish Red Teams to challenge aspects of their own plans, programmes and assumptions. It is this aspect of deliberate challenge that distinguishes red teaming from other management tools, although there is not a sharp boundary between them. Nowadays, red teaming often comes from an intelligence-led penetration testing approach, designed to more thoroughly test an organisation’s defences in real-world scenarios.

Blue Teaming focuses on the defensive role of an organisation, rather than on developing methods of attacking an organisation.

Blue Teams are usually proactive internal security teams that defend against both real attackers and Red Teams. Blue Teams are different to standard security teams in most organisations. Most standard security operations teams do not have a ‘constant vigilance’ mentality against attack, which is the mission and perspective of a Blue Team. There are several proactive roles that a Blue Team can fill, including configuring Security Operation Center (SOC) evaluations, technical security evaluations, patch management reviews and other elements. This helps remove easy-to-find security issues, enabling the penetration testing team to concentrate on finding the more in-depth issues, thereby making best use of resources. **Purple teams** exist to ensure and maximise the effectiveness of the Red and Blue teams. They do this by integrating the defensive tactics and controls from the Blue Team with the threats and vulnerabilities found by the Red Team into a single narrative that maximises both. Ideally Purple shouldn’t be a team at all, but rather a permanent dynamic between Red and Blue.

Organisations should consider the need for both Red and Blue Teaming as part of their penetration testing programme.

Many CREST members are at the cutting edge of both Red and Blue Teaming and are well positioned to offer world-class testing services.



Part 3 – Preparing for penetration testing

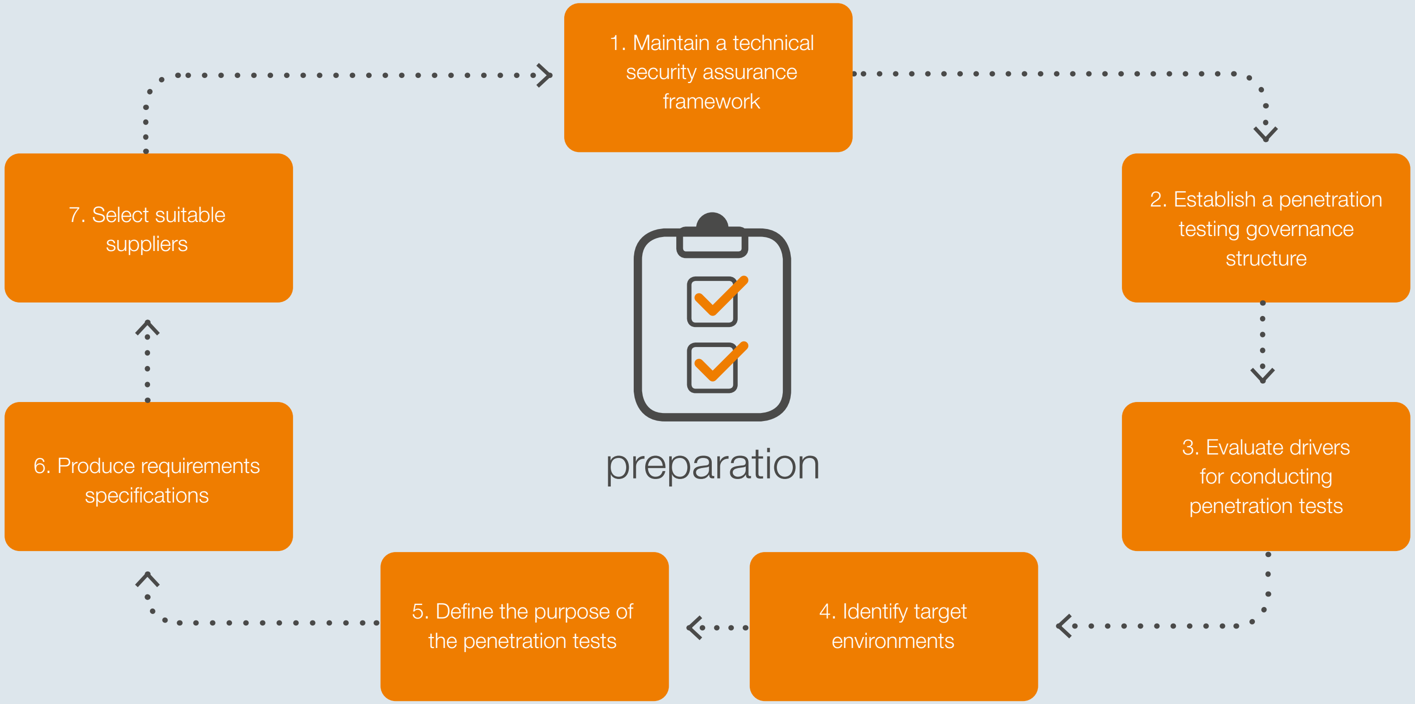
Overview

A senior management team should be appointed with responsibility for establishing and overseeing an enterprise-wide penetration testing programme and ensuring it meets business requirements.

To be effective, your penetration testing programme must include all relevant aspects of preparing for penetration tests, carrying them out in practice and ensuring follow-up activities are undertaken, including remediation processes and security improvement action plans.

The preparatory steps required are outlined here, in Figure 3:

Figure 3: Key steps in the preparation phase



1. Maintain a technical security assurance framework
2. Establish a penetration testing governance structure
3. Evaluate drivers for conducting penetration tests
4. Identify target environments
5. Define the purpose of the penetration tests
6. Produce requirements specifications
7. Select suitable suppliers

Each step is explained in more detail on the following pages.

1. Maintain a technical security assurance framework

Your organisation should maintain an approved technical security assurance framework, which is focused on protecting your most critical information and systems.

A technical security assurance framework would typically include multiple environments for testing, a security architecture, an on-going security monitoring services (e.g. in a SOC), an adequate range of technical security services and a balanced selection of preventative, detective and reactive security controls. These must be supported by sufficient budget, skilled resources, processes, tools and technology, adequate management support and an IT or cyber security risk management programme.

All main internal systems that support your organisation should be identified. Details of these internal systems should be recorded in a registry or equivalent, such as an asset registry or a Configuration Management Database (CMDB).

Records about the systems and processes that need to be maintained include:

- Their level of criticality to the business
- The sensitivity of any information they handle (e.g. via an information classification scheme)
- Any key dependencies (e.g. on other systems or networks, information feeds, physical equipment)
- Network diagrams, data flows and trust boundaries
- Details about important third-party suppliers
- IT infrastructure
- Points of contact, roles and responsibilities

Different levels of security assurance should be applied to different systems based on their criticality or the sensitivity of the information they handle.

To support these records, you should identify and categorise all main third party:

- Systems that could be utilised to compromise the technical security environment of your organisation
- Functions from which information could be obtained to mount a social engineering attack on the business

Cyber security incident response capability

A critical part of an organisation's defences against cyber security attacks is a robust, well-thought out cyber security incident response capability, which often has close links to penetration testing approaches and red teaming exercises.

CREST has produced a useful **Cyber Security incident Response Guide**, supported by a suite of spreadsheet-based maturity assessment tools (including high level and detailed **Cyber Security Incident Response Maturity Assessment** tools), both of which are available, free-of-charge, at: **www.crest-approved.org**.

An underlying technical security assurance framework should be maintained to support important internal and third-party systems. The framework must be reviewed and approved by appropriate business and IT management. Your technical security assurance framework should include:

- Multiple environments for testing (eg. development, staging and live)
- A security architecture
- A balanced selection of preventative, detective and reactive security controls
- An on-going security monitoring service, for example as part of a Security Operations Centre (SOC)
- An adequate range of technical security services (e.g. malware protection, traffic filtering and intrusion detection systems)
- Continuous vulnerability assessment
- Methods of collecting, interpreting and acting upon appropriate sources of threat intelligence
- A road map or similar to provide a short, medium and long term outlook for security posture

Your technical security assurance framework should include testing:

- Backups, to ensure critical information and systems can be restored within critical timescales
- Incident response processes
- Disaster recovery / fail-over processes

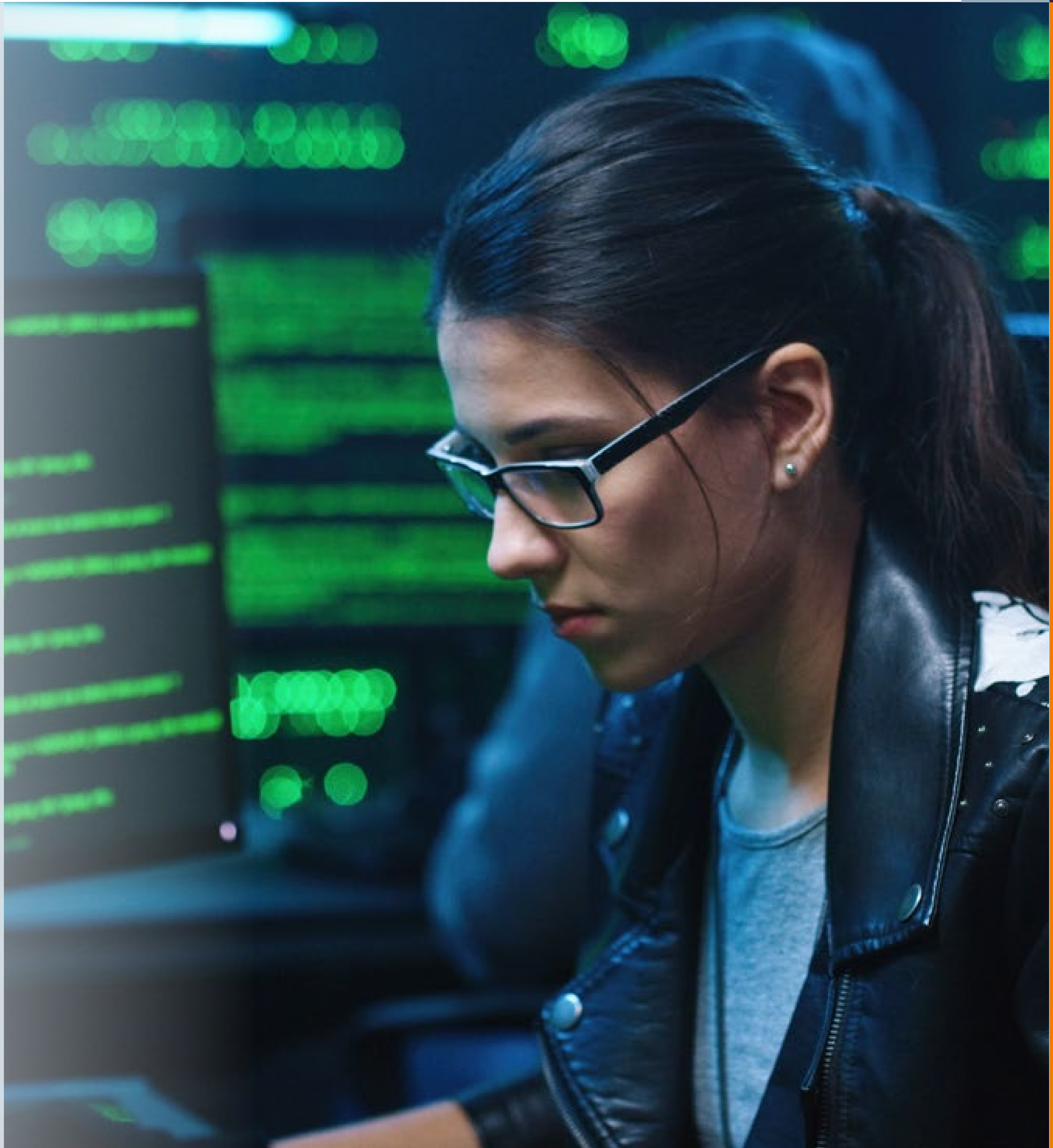
Your technical security assurance framework should be supported by sufficient budget, skilled resources, processes, tools and technology.

A technical security assurance framework should receive adequate management support in terms of:

- Co-operation, authority and escalation processes
- Integration into your procurement process
- Performing regular penetration testing of key elements
- Independent review

It must also be supported by an information, IT or Cyber security risk management programme, which should include:

- Details of your organisation's primary concerns for protecting the confidentiality, integrity and availability of information and supporting systems (e.g. in a documented risk appetite statement)
- An up-to-date list of all relevant legal, regulatory and contractual compliance requirements
- A list of all main threats
- A risk register showing exposure of key assets
- A method of assessing the effectiveness of technical security arrangements



2. Establish a penetration testing governance structure

Your organisation should establish a suitable governance structure to oversee and co-ordinate a regular penetration testing programme.

An effective governance structure for penetration testing would typically:

- Cover all main systems enterprise-wide (while focusing on the most critical), through a penetration testing programme that includes penetration testing processes and methodologies, supplier selection criteria, and a penetration testing assurance management framework
- Be supported by a joint management and technical team to agree the programme and scope of regular penetration testing, an effective change management process and a set of key performance indicators for penetration test results

The governing management and technical team should have:

- Direct access to senior management to raise significant concerns
- The ability and authority to contribute to a wider security improvement plan
- Adequate control over the penetration testing programme

Scoping the penetration testing programme

The scope of your penetration testing programme should:

- Cover all main systems, enterprise-wide
- Focus on critical systems
- Allow for protection of sensitive information

It should include:

- A set of penetration testing processes and methodologies that apply enterprise-wide
- Supplier selection criteria
- A penetration testing assurance management framework
- Follow up activities to ensure that remediation activities are carried out in an effective manner, reducing the risk of vulnerabilities being exploited in the future

A penetration testing programme should be:

- Approved by appropriate business and IT management
- Supported by stated objectives and timelines
- Integrated into your underlying technical security assurance framework
- Reviewed regularly and kept up to date

The programme should align within:

- A wider security review framework (eg. ISO 27001, the US Department of Commerce's National Institute of Standards and Technology (NIST) **cyber security framework**, ISF Standard of Good Practice)
- Technical security infrastructure (including on-going security monitoring, vulnerability assessment, malware protection and patch management)
- System development processes (particularly for Web applications)

Controlling changes to the penetration testing programme

There should be a mechanism for applying controlled changes. This change management process should enable the secure introduction of new:

- Business initiatives (e.g. new business models, international expansion, mergers and acquisitions)
- Business processes
- Web applications, and
- IT infrastructure

The change management process should include making changes in a secure manner to:

- Existing business processes or applications
- Legal and regulatory requirements
- Security services, such as a Public Key Infrastructure (PKI), malware protection software, and Intrusion Detection Systems (IDS)

This process should also include making changes in a secure manner to your organisation's:

- Threat landscape
- Security governance approach (e.g. a new security organisation set up or risk management programme)
- Security controls framework (e.g. based on ISO 27001, COBIT 2019, the **SANS CIS Controls** or the ISF Standard of Good Practice)

Supporting the penetration testing programme

To support your penetration testing programme, you should maintain key performance indicators for penetration test results that can be used to help establish the 'health' of the overall business. Subscribing to information sharing platforms or services, locally, regionally and internationally will help in knowledge sharing and current threat awareness. Using information sharing platforms or services, this intelligence can then feed into the penetration testing programme.

The suitability and effectiveness of your penetration testing programme should be assured by:

- Traceability and monitoring of the programme
- A continuous improvement process
- Regular management and technical review, and
- Independent audits (or similar)

3. Evaluate drivers for conducting penetration tests

Your penetration testing programme should include evaluating drivers for carrying out penetration tests as part of a technical assurance programme, based on evaluation of relevant criteria, such as the impact of serious incidents, increased threat levels or significant changes to business or IT processes.

Organisations may have many different drivers for undertaking penetration tests of their critical business applications or infrastructure. Whatever the drivers are for testing in your organisation, it is important to determine what penetration testing will help you achieve.

Drivers for carrying out penetration tests should be based on evaluation of relevant criteria, which could typically include:

- A growing requirement for compliance
- The impact of serious (often cyber-related) security attacks on other similar organisations
- Use of more outsourced services
- The introduction of new – or significant changes to – important operational processes
- Major change to business applications or IT infrastructure
- Changes in the perceived threat (e.g. based on single point or continuous threat monitoring)
- A need to perform an independent assessment of your security arrangements (for example, due to legal / regulatory or customer requirements

Drivers for penetration testing should take account of:

- How a penetration test fits into your organisation’s overall security arrangements
- The nature and direction of your business – and your risk appetite
- The benefits of adopting a systematic, structured approach to penetration testing
- Findings from risk assessments, audits or reviews carried out by specialists in information security assessments, risk management, business continuity, internal audit or insurance
- Overall compliance requirements, not just those directly mentioning penetration tests
- Analysis of security incidents that have taken place both in your own organisation and in similar organisations
- Lessons learnt from previous penetration tests conducted in your organisation

Penetration tests carried out in isolation can derive a good understanding of technical risks and identify security improvements. However, If the testing can be placed within a wider framework of security assessment and strategy, this helps contextualise findings and recommendations.

Drivers for penetration testing should be defined to help:

- Support adoption of a strategic view of security management
- Ensure major system vulnerabilities are identified and addressed
- Reduce risk of discovering the same problems still exists (or exists on a similar system) the next time a penetration test is carried out

4. Identify target environments

Your penetration testing programme should include clear identification of target environments that need such testing. When identifying target environments, you should consider the need to carry out penetration testing on:

– Important business processes
– Critical web applications
– Key parts of IT infrastructure (eg. a major data centre or the corporate network)
– Specialised equipment (eg. mobile devices and process control systems)
– Relevant system development lifecycles

Identification of target environments that need to be subject to penetration testing should take account of a wide range of factors including:

- The criticality of the system to your organisation (often identified by performing a critical function or business impact assessment)
- Regulatory and compliance requirements, such as the **Payment Card Industry Data Security Standard** (PCI DSS)
- Major business or IT changes
- Critical systems under development
- Outsourced applications or infrastructure (including cloud services)
- Any wider technical security assurance programme

Criticality

To identify the most critical systems, your organisation should consider the:

- Nature of business being conducted
- Size of the target systems – and the sensitivity of data associated with the systems
- Sensitivity of data associated with the target environment
- Potential business impact if that system were to be compromised – and the likelihood of it actually being compromised

For some organisations, the first step in procuring a penetration test is to conduct a risk assessment of assets. This helps ensure testing will focus on the assets that pose the highest risk.

Compliance

Some industries and data types are regulated and must be handled securely (like the financial sector, or credit card data). In this case, your regulator will insist on a penetration test as part of a certification process. Some industry standards, such as ISO 27001 and PCI DSS, also specify the requirement for penetration testing.

"Compliance is a different beast to security and exists separately. It is possible to be compliant, yet not secure; and relatively secure, but non-compliant."

Major changes

Most organisations in today's dynamic world make significant changes on a fairly regular basis – to business processes, applications, IT systems or end user environments, to name a few. Many changes can have a significant impact on threat profile and security arrangements. It is important, therefore, to carry out a penetration test immediately following a major change to the system or the business environment it supports.

Systems under development

Often the decision to conduct independent penetration testing on a new system comes late in the project lifecycle. As a result, there is often insufficient budget for desired testing, very limited time before the system needs to go live and little ability to change the system as a result of any security vulnerabilities identified. Security testing should be fully incorporated into your system development lifecycle (SDLC) – as outlined in the table below – and not just conducted as a "tick box" exercise near project completion.

SDLC stage	Actions to consider	To ensure that…
1. Planning and requirements	Build independent penetration testing into requirement specifications – allocating sufficient funding and resources – and schedule at key points	Business and security requirements are met
2. Design	Engage with a penetration testing supplier to define scope and incorporate this into your project plan – and to conduct threat modelling exercises	Penetration testing is baked into the design process
3. Development	Integrate penetration tests into your traditional security testing approaches, including source code review	Coding weaknesses are identified as soon as possible
4. Integration and test	Perform vulnerability scanning and build reviews	System builds are secure
5. Implementation	Conduct exploitation testing of applications and networks	Vulnerabilities are addressed
6. Maintenance	Subject critical systems to regular penetration testing (at least yearly) – and after any major change	Systems are as well protected as possible

Security testing should include consideration of changes to the level of threat, which would mean an increase in the level of vigilance, validation of controls and nature of penetration testing. This provides greater technical assurance against cyber security attacks and a heightened level of cyber security awareness.

Outsourcing

Many organisations place a great deal of reliance on outsourced services (often to cloud service providers). But attacks are not constrained by whether the business manages its own environment or not. Obviously, any weaknesses in the security of outsourced third parties can significantly impact your IT security.

If you are not permitted to test an important environment controlled by a third-party, you should seek assurances that:

- Appropriate penetration tests are regularly carried out
- These tests are conducted by suitably qualified staff working for a certified organisation
- Test recommendations are acted upon

5. Define the purpose of penetration tests

Your penetration testing programme must include defining the purpose of your penetration tests and evaluating potential benefits of these tests to your organisation.

To identify the purpose of penetration tests, ask whether these tests can help your organisation to meet requirements and realise potential benefits – while taking into account any testing limitations or difficulties.

When defining the purpose of your penetration tests, you should assess whether these tests can help:

- Identify weaknesses in your security controls
- Enable the business (particularly for electronic commerce)
- Reduce the frequency and impact of security incidents
- Comply with legal and regulatory requirements (e.g. PCI / DSS, NERC, ISO 27001, HIPAA or FISMA)
- Provide assurance to third parties that business applications can be trusted, and that customer data is adequately protected
- Limit liabilities if things go wrong, or if there is a court case (ie. take 'reasonable' precautions)

"We suspected we had already been hacked and wanted to find out more about the threats to our systems, to help reduce the risk of another successful attack."

Another purpose for conducting a penetration test can be to limit liabilities if things go wrong, or if there is a court case.

You should determine what business benefits penetration testing will help you achieve.

When identifying and evaluating the potential benefits of effective penetration testing, consider:

- A possible reduction in long-term ICT costs
- Improvements in your technical environment, reducing support calls
- Greater levels of confidence in the security of your IT environments
- Increased awareness of the need for appropriate technical controls

You should also consider the limitations of penetration testing, taking into account the points raised on Page 11.

As well as considering any limitations, you should evaluate the potential difficulties involved with carrying out penetration testing, which can include the difficulties already identified on page 11, but also:

- understanding the costs of external services – and determining the true overall cost of testing, and
- finding a suitable penetration testing expert when required, often at short notice

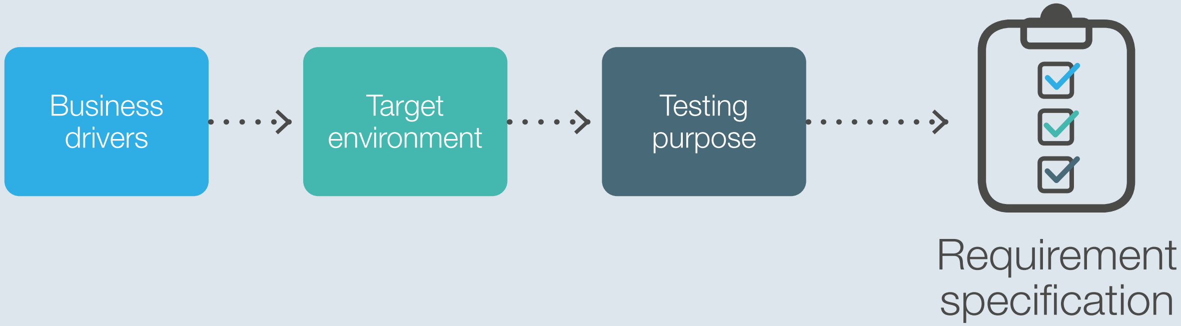
6. Produce requirements specifications

Requirements for penetration testing should include consideration of important business applications, key IT infrastructure and confidential data, validation that tests are legal and will not compromise confidential data and the need for tests to be recorded, reviewed and signed-off.

There will often be a trigger that causes you to carry out a penetration test (or a series of tests), possibly due to being informed about a need for compliance or as a result of an incident.

It can be tempting to immediately start thinking about getting an external supplier to come in straight away and start testing. But in reality, a more effective approach is to determine your business requirements for penetration testing first, and then consider the best way these requirements can be met. The key elements of a possible approach are shown in Figure 4, below.

Figure 4: A process for specifying penetration testing requirements



Requirements for penetration testing should specify:

- The scope of testing (e.g. a critical web application or important IT infrastructure)
- What will be specifically excluded from the testing scope, and
- How regularly the penetration testing is carried out

Your requirements for penetration testing should include considering potential impact on:

- Important business applications
- Key systems and networks (IT infrastructure), and
- Confidential data

Requirements for penetration testing should specify testers must validate:

- The test will be legal
- The test will not compromise data protection requirements
- They have the relevant qualifications and experience to perform required testing to the required standard
- They will act in a professional manner (e.g., in line with a reputable code of conduct)

Requirements should be:

- Formally recorded in a requirements specification
- Formulated and reviewed by competent technical experts
- Reviewed by business management
- Signed-off by senior management
- Monitored to ensure they are met
- Reviewed and revised on a regular basis

Requirements for penetration testing should take account of the benefits of using external suppliers.

7. Select suitable suppliers

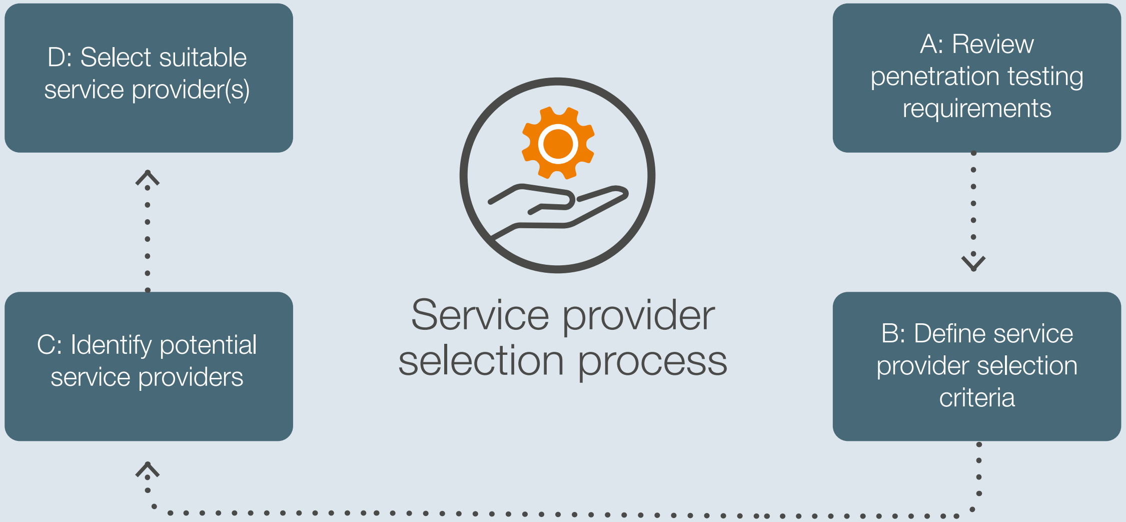
Your programme should include appointing suitable third-party suppliers to undertake independent penetration testing of target environments, based on defined requirements, benefit evaluation, specified supplier selection criteria and validation of the supplier's ability to meet your specific requirement.

Effective supplier selection criteria should be used to determine if potential suppliers can meet your testing requirements, based on their ability to provide:

- Solid reputation
- History and ethics
- High quality, value-for-money services
- Research and development capabilities
- Highly competent, technical testers, and
- Security and risk management, supported by a strong professional accreditation and complaint process

"What we are looking for from a supplier is certainty, prioritisation, trust and security."

Figure 5: The service provider selection process



A: Review penetration testing requirements

B: Define service provider selection criteria

C: Identify potential service providers

D: Select suitable service provider(s)

Service provider selection process

A typical service provider selection process is outlined in Figure 5 below.

When appointing an external penetration service provider, choose a supplier who can meet your requirements in the most appropriate manner – at the right price.

"It is important to ensure that the right systems are being tested by the right people for the right reasons at the right time."

A. Review requirements

Make sure that whoever chooses the supplier fully understands your organisation's requirements and is aware of any necessary management, planning and preparation activities. Much of this should be determined in the requirements stage of the procurement approach, but will be vital in procuring the right service from the most appropriate supplier.

You should consider who is driving the relationship with the supplier within your organisation. It is seldom a good idea to just leave it to a corporate procurement person as this is unlikely to deliver maximum value. From interviews with service providers, when clients have used a security or compliance person to drive the relationship, this has typically produced better results.

Your requirements for penetration testing suppliers should be:

- Formally defined
- Based on a cost / benefit analysis
- Driven by clear objectives
- Recorded in a requirements specification, and
- Integrated into your organisation's procurement process

Some organisations seem to believe that they just need a ‘tick in the box’ and may be looking for a ‘cheap and dirty’ solution. However, this often does not produce required results and may even create a false sense of security. It can also cause difficulties during the procurement process as quality suppliers will believe in performing a proper test.

In addition to defined business requirements and an agreed scope statement, there may be other considerations when selecting a supplier. For example, you may have a well-established (or preferential) relationship with a particular supplier or a need to appoint (or reject) another potential supplier for commercial or political reasons.

When appointing external suppliers – for any purpose – you will sometimes have to take into account topics covering political, legal / regulatory, socio-economic and technological (PLEST) issues.

Your requirements can also be influenced by the size (and bargaining power) of your organisation, and the market sectors in which you operate.

When evaluating the benefits of external suppliers, you should consider their ability to:

- Deploy a structured penetration testing process and plan, developed by experts
- Specify the purpose and scope of tests
- Increase the scope and frequency of tests
- Conduct short term engagements, eliminating the need to employ your own specialised (and often expensive) staff, reducing the cost of training internal teams
- Take advantage of automation (e.g. by using penetration testing workflows and importing vulnerability management reports)

B. Define supplier selection criteria

To ensure your chosen supplier will meet requirements, it can help to define a set of supplier criteria, most of which it should be able to meet – or exceed. Potential suppliers should be able to:

- Provide a reliable, effective and proven penetration testing service at a reasonable price, within specified timescales
- Meet compliance standards and the requirements of corporate or government policy, protecting client information and systems both during and after testing
- Perform rigorous and effective penetration tests, ensuring a wide range of system attacks are simulated
- Adhere to a proven testing methodology, allowing sufficient time for remediation
- Carry out a full range of testing (e.g. black-, white- or gray box, internal or external infrastructure or web application, source code review and social engineering)
- Discover all major vulnerabilities, identify associated ‘root causes’ and strategically analyse key findings in business terms
- Co-develop security improvement strategies and programmes, recommending countermeasures to both address vulnerabilities and prevent them from recurring
- Produce insightful, structured, practical and easy to read reports, engaging with senior management in business terms, resolving issues with IT service providers, and addressing global risk management issues
- Provide on-going advice on how to manage systems effectively over time as part of a trusted relationship

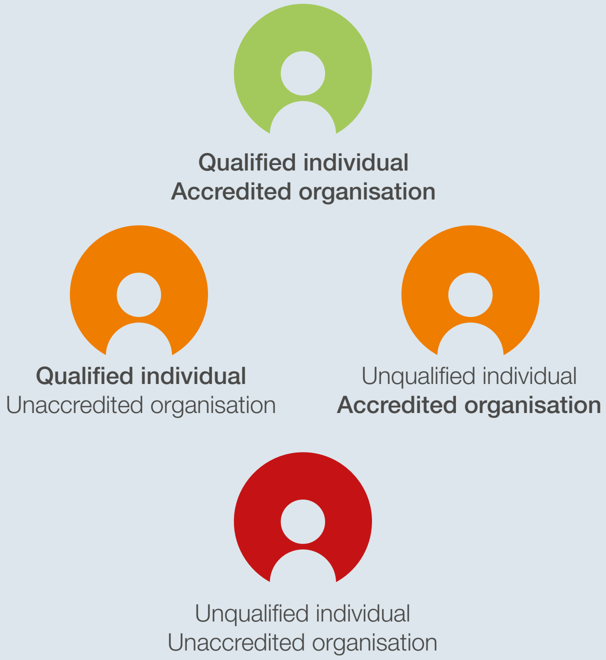
Your supplier selection criteria should be recorded in a document that can be passed to potential suppliers – and your procurement department – sometimes as part of an RFP (Request for Proposal).

Professional accreditation

In some cases, penetration testing service providers are also accredited to particular schemes, but do not use qualified individuals to conduct penetration testing. So, the required testing quality may not be achieved. In other cases, an individual may be qualified, but does not work for an accredited organisation, meaning there are fewer assurances about protection of confidential information or the overall quality of the service provided. Complaints may be more difficult to resolve.

The optimum combination is shown in green in Figure 6 below. This is the only combination that provides you with a tangible level of protection should things go wrong – and reduces likelihood of a problem occurring in the first place.

Figure 6: Combinations of accreditation for organisations and the individuals they employ


Qualified individual
Accredited organisation
Qualified individual
Unaccredited organisation
Unqualified individual
Accredited organisation
Unqualified individual
Unaccredited organisation

Although value can be obtained by appointing either qualified individuals or accredited organisations, it is the combination of these that will provide you with the greatest assurance that the most effective tests will be conducted – and in the most professional manner.

By procuring penetration testing services from qualified individuals who work for trusted organisations, you can rest assured that an expert and independent body – with real authority – is on hand to investigate any complaint thoroughly and ensure a satisfactory conclusion is reached.

> **"CREST provides demonstrable assurance of the processes and procedures of member organisations and validates the competence of information security investigators."**

By using a supplier which is a CREST penetration testing services accredited member, you gain reassurance that:

- You are dealing with a trusted organisation in a relatively new area
- It has signed up to an independent code of conduct
- A proven penetration testing methodology will be adopted
- Its processes and procedures will have been subject to independent vetting
- Your systems and data will be handled carefully, in a professional manner
- The penetration testing itself will be kept confidential
- Advice will be given on how to reduce the likelihood of similar vulnerabilities being exploited

Independent complaints process

Appointing suppliers that are members of a professional penetration testing body can provide you with a reliable and proven complaint process (including constructive advice), as shown in Figure 7 below.

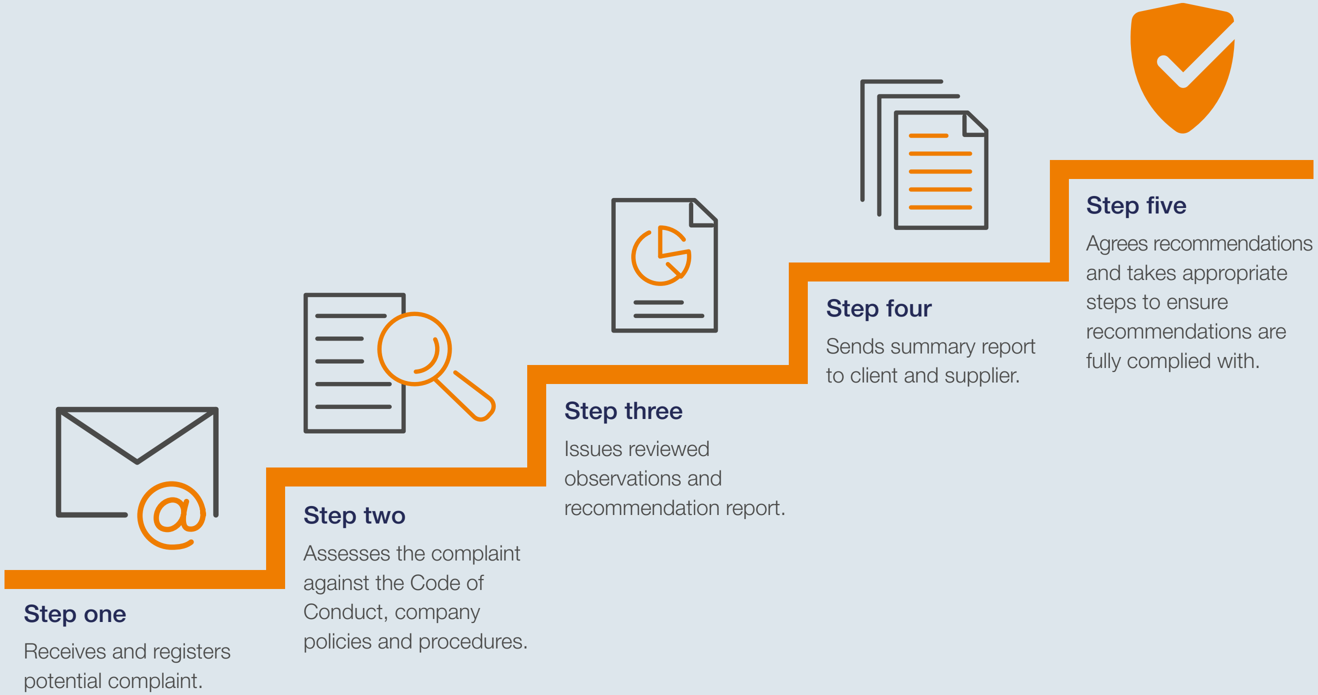
If there are any problems with the quality of work done, or approach taken by the penetration testing team (including investigators, analysts and recovery experts), you can rest assured an expert and independent body is on hand to investigate any complaint thoroughly and ensure a satisfactory conclusion is reached.

A CREST penetration testing member can expect to receive severe penalties if they do not:

- Adhere to the **CREST Code of Conduct**
- Act in a professional, ethical manner
- Ensure its recovery team and ancillary staff comply with its submitted and reviewed policies, processes and procedures to protect client information

CREST penetration testing members can have their membership revoked if they do not meet required standards, or have been proven, in an investigation, to have acted in a significantly negligent or unethical manner. In the worst case, this could result in a significant reduction in business, as clients would not be prepared to procure their services.

Figure 7: Typical complaint handling process for a professional body


Step one
Receives and registers potential complaint.
Step two
Assesses the complaint against the Code of Conduct, company policies and procedures.
Step three
Issues reviewed observations and recommendation report.
Step four
Sends summary report to client and supplier.
Step five
Agrees recommendations and takes appropriate steps to ensure recommendations are fully complied with.

C. Identify potential service providers

It can often be difficult to produce a short list of potential suppliers, not least because there are so many to choose from. For example, penetration testing suppliers can include:

- Organisations specialising in penetration testing (often small boutique firms)
- Information security consultancies and integrators, with penetration testing teams
- Systems integrators and outsourcing service providers with penetration testing teams
- Regulated professional services firms, including the 'Big 4' accountancy firms, with penetration testing teams

To help identify potential suppliers, you may wish to carry out some background research to see if they have:

- Carried out the type of testing you require
- Received positive feedback from previous clients
- Taken part in specialised industry events, such as those run by CREST or Open Web Application Security Project® (OWASP) chapters
- Produced research papers, published vulnerabilities or won industry awards
- Valid accreditations and qualifications
- Membership of a professional penetration testing body, such as CREST
- Complied with appropriate vetting standards, such as the BSI security screening of employees (BS7858, or equivalent)
- Been audited (e.g. by some of their larger clients), to provide assurance for their wider client base

As part of your supplier selection process, you should:

- Produce a short list of potential suppliers, based on evaluation of at least three different suppliers
- Validate the ability of potential suppliers to meet your specific requirements (not just one who can offer a variety of often impressive products and services, some of which may not necessarily be relevant)

You should ensure that your chosen suppliers are able to:

- Effectively meet – or exceed – your supplier selection criteria
- Provide tangible value for money

D. Appoint suitable suppliers

After carefully considering all the relevant supplier selection criteria – and evaluating potential suppliers – you will then need to go through a formal, approved appointment process for selected penetration testing suppliers.

The key consideration should still be to select a supplier who can help you meet your specific requirements – at the right price – not just one who can offer a variety of often impressive products and services, some of which may not necessarily be relevant.

Prior to work starting, arrangements with your chosen supplier should be satisfactorily detailed in a contract signed off by both parties

The appointment and continued use of external providers can be managed in a number of ways that can be tailored to fit an organisation's style. Use of penetration testing providers tends to fall into the following models, right:

Supplier appointment model	Advantages	Disadvantages
Single provision – a single provider is used for all penetration testing.	This can provide an extensive relationship where the supplier is very familiar with your organisation and can therefore provide insightful and practical recommendations.	A single supplier may not be able to provide all types of penetration testing equally well. In addition, over-familiarity may give rise to conflicts of interest.
Dual provision – two suppliers are used. Penetration tests are assigned according to the technical speciality of the supplier (eg. one supplier for infrastructure testing and one for application testing).	This retains the benefits of single provision while also playing to the strengths of the providers.	The possibility of over-familiarity remains with this model, and there may be additional cost associated with suppliers having to gain background information on the target systems.
Testing panel – multiple suppliers are used. Penetration tests are either assigned in a cyclic fashion or according to technical speciality.	Over-familiarity is less of a possibility and subsequent penetration tests on systems can be performed by different providers to make testing more thorough.	The selection, contract maintenance and test management can be complex and expensive.
Ad-hoc – various suppliers are used, dependent on the particular penetration test being performed.	This model allows for flexibility and the ability to specifically select suppliers based on their capability.	Suppliers are likely to have little or no familiarity with systems.

Some organisations choose to rotate vendors, with a timescale dependent on the type and number of tests to be performed.

Tests are often carried out on a regular (typically annual) basis. However, they are often more effective if carried out immediately before (or after) a major change – often saving money in the longer run, too.

Part 4 – Conducting penetration tests

Overview

A detailed test plan should be produced that outlines what will actually be done during the test, often as series of discrete tasks. This test plan should identify the processes, techniques or procedures to be used during the test.

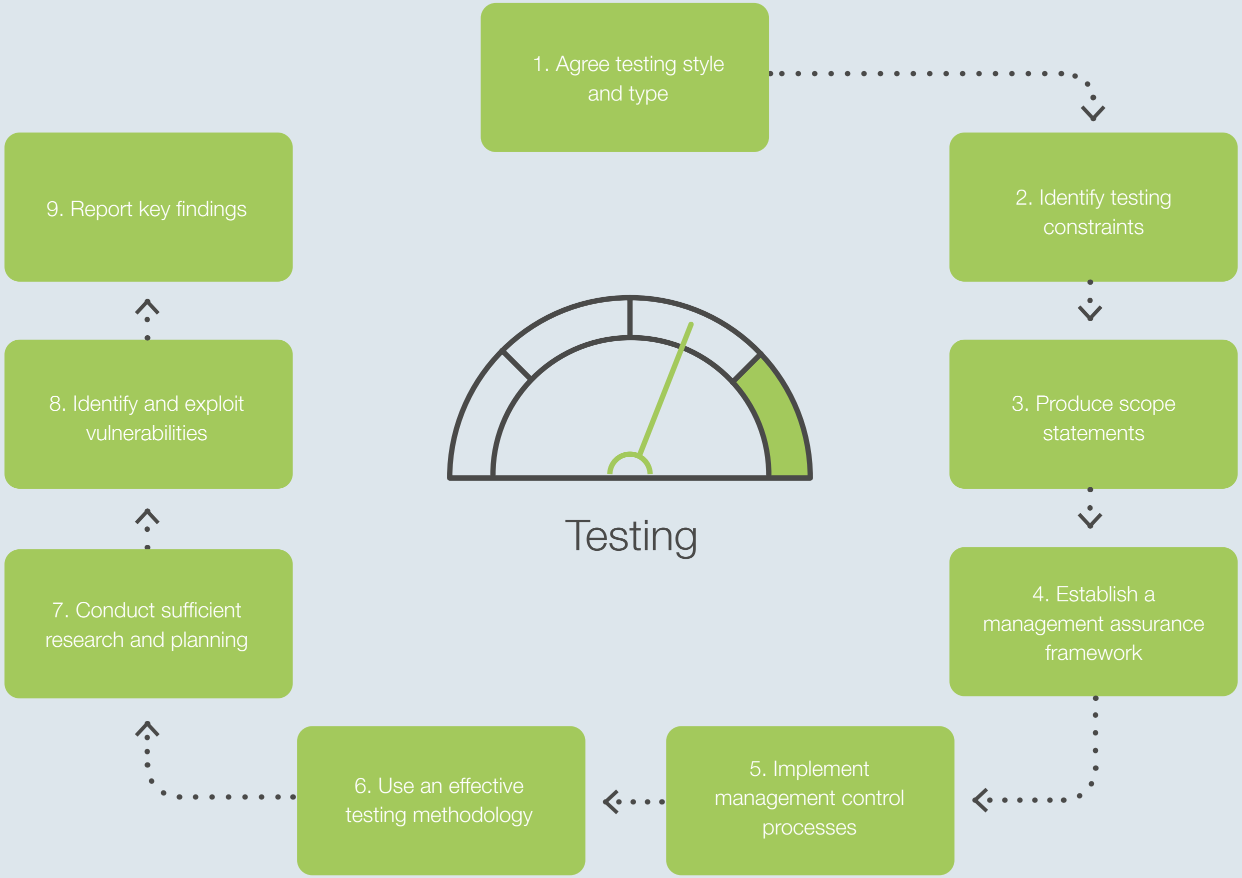
Findings identified during the penetration test should be recorded in an agreed format describing each finding in both:

- Technical terms that can be acted upon
- Non-technical, business context, so that justifications for corrective actions are understood

Steps that need to be taken for each individual penetration test performed as part of the enterprise-wide penetration testing programme are outlined in Figure 8, right.

Some of these steps will need to be repeated when testing target systems, particularly steps 7 and 8, dependent on scope and requirements.

Figure 8: The penetration testing process


1. Agree testing style and type
2. Identify testing constraints
3. Produce scope statements
4. Establish a management assurance framework
5. Implement management control processes
6. Use an effective testing methodology
7. Conduct sufficient research and planning
8. Identify and exploit vulnerabilities
9. Report key findings
Testing

Each step is explained in more detail on the following pages.

1. Agree testing style and scope

Your penetration testing programme should include determining what style of penetration testing is required (e.g. black, gray or white-box testing; internal or external testing) and what type of testing is to be performed.

Style of testing

Black-box security testing refers to a method of software security testing in which the security controls, defences and design of an application are tested from the outside-in, with little or no prior knowledge of the application's internal workings. Essentially, black-box testing takes an approach similar to that of a real attacker.

White box testing is a security testing method that can be used to validate whether code implementation follows intended design, to validate implemented security functionality, and to uncover exploitable vulnerabilities.

Gray-box testing splits the difference between white-box and black-box testing. By providing a tester with limited information about the target system, gray-box tests simulate the level of knowledge that a hacker with long-term access to a system would achieve through research and system footprinting.

Careful consideration should be given to the style of testing required, such as black, gray or white-box testing.

Testing style	Overview	Useful to…
'Black box'	No information is provided to the penetration tester	Simulate external attacks with no prior knowledge of the target environment – and understand what is possible for an uninformed attacker to achieve.
'Gray box', also known as 'translucent box'	Limited information is provided, e.g. login credentials to a system or visitor access to a site	Understand the degree of access that authorised users of a system can obtain – and the possible damage caused by insider or privileged attacks with some knowledge of the target environment.
'White box' – also known as 'crystal' or 'oblique' box'	Full information is provided, for example network maps and access to development staff	Support a more targeted test on a system that requires a test of as many vulnerabilities and attack vectors as possible.

Black box testing can be a little misleading. For some system attacks a determined attacker would do so much reconnaissance that they would have virtually the same knowledge as an insider anyway.

Findings from the research project revealed a majority of supplier's clients specify white- or gray-box testing, rather than black-box testing. Many clients simply ask a supplier to run a 'typical' penetration test, which nearly always involves gray-box testing.

White-box testing can be less authentic as an attack, but is a much more effective use of a penetration tester's time, reducing cost to your business. The more traditional black-box testing is still undertaken, but this tends to be for a specific purpose.

Testing can be carried out either at a supplier's premises or at a client's location (or a little of both).

- An 'external' penetration test is the most common type of test and is aimed at IT systems from 'outside the building', testing systems that are 'internet connected', such as the Demilitarised Zone (DMZ) of your network, Virtual Private Networks (VPN), and your websites
- An internal security test (sometimes replicated by a supplier on their own site, maybe in a laboratory) focuses on what staff can see and do within their own IT network, and is typically associated with white- or gray-box testing

Type of testing

The scope of the test should identify what type of testing is to be performed, such as web application testing (which finds coding vulnerabilities), or infrastructure testing (which examines servers, firewalls and other hardware for security vulnerabilities).

Some organisations classify applications (in terms of criticality) as high, medium or low value applications – and test accordingly. Infrastructure testing is often carried out on a regular cycle or after a major change.

Other forms of system penetration testing are also conducted, such as for mobile, client server or cloud-based applications; user devices, including workstations, laptops and consumer devices (eg. tablets and smartphones); and wireless – but typically the same penetration testing principles apply.

When conducting penetration tests, you should consider the use of end-to-end testing (i.e. for people, through data, devices, applications and infrastructure), emerging technologies (e.g. mobile applications) and social engineering.

For optimum results, the penetration test should be conducted in the live environment. However, this not always possible (or advisable), so testing is often carried out in a 'test' environment. Testing activities conducted in a 'test' environment:

- Allow more disruptive or destructive testing to be performed, such as 'denial of service' type tests or the use of exploits against vulnerabilities
- Are unlikely to affect users of 'live' systems, so there will be no business impact
- Should be as similar to the live environment as possible

2. Identify testing constraints

Your penetration testing programme should include identifying any testing constraints associated with planned penetration testing.

There are always constraints with any form of testing and penetration testing is no exception. Tests are often constrained by aspects of the business that cannot be tested due to operational and technical limitations, legal restrictions and the lack of time and resources to carry out testing on a continual basis.

Testing constraints need to be identified and adhered to, while ensuring real world scenarios are adequately tested.

The table, right, outlines common penetration testing restrictions, highlighting potential implications for malicious attackers and presenting actions to consider for addressing these issues.

Constraint on tester	Implication for attackers	Actions to consider
There are typically aspects of the business that cannot be tested due to operational limitations.	Attackers often do whatever it takes to penetrate an organisation or system. If they are not able to penetrate a particular system, they may simply try another route.	Simulate live tests as closely as possible. Conduct tests outside of normal hours (and locations).
Testing must be conducted within the confines of the law.	Attackers will often break the law to achieve their objectives.	Tailor the way tests are structured and run to simulate most forms of attack. Take back-ups of critical systems and files before testing.
Testers are limited to the scope of the testing – they are unlikely to be allowed to utilise business partners, customers or service providers as a platform from which to launch an attack.	Attackers will utilise the weakest point of security in any part of connected systems or networks to mount an attack, regardless of ownership, location or jurisdiction.	Include perimeter controls within the scope of the test. Apply more rigorous testing to applications that are accessible from outside the boundaries of the business.
Limited time to conduct tests.	Attackers have unlimited time to mount a concerted attack against a system if they have the motivation, capability and resources to do so.	Invest more time in testing critical systems. Provide testers with as much background information as possible, reducing reconnaissance time and thereby increasing testing time.
Any test is only a snapshot in time, and changes to the threat or the environment could introduce new vulnerabilities.	Attackers can attack the environment at any time.	Conduct penetration testing on a regular basis, rather than as a one-off exercise.

Bearing in mind these testing constraints, penetration testing should not be assumed to find all vulnerabilities of given systems or environments. The law of diminishing returns often applies in that the most obvious vulnerabilities will be discovered first, with further time yielding more and more obscure issues. Consequently, it is often advisable to adopt a 'risk to cost balance' when performing tests.

Simply fixing vulnerabilities uncovered during testing could leave a number of other vulnerabilities present for an attacker to find – emphasising the need to employ competent professional penetration testers.

Technical considerations

To carry out the most effective penetration testing, the environment being tested should be as close to the live environment as possible. However, there are often technical issues that need to be considered that can affect the scope of the test or the security countermeasures in place to detect and deter attacks. As an example, two of the most common of these technical considerations are outlined in the table below:

If you have…	You may need to…
IDS / IPS deployed within your environment	Implement policy exceptions and ensure they do not significantly block testing
Network or web application firewalls deployed	Be aware that vulnerabilities present in your servers or application will not be discovered if the testing is undertaken from outside your network

There may be many other technical considerations that are specific to your environment. Key points to remember are that you should:

- Define how testing will be conducted during the scoping phase
- Ensure the scope is practical and that testing will meet your requirements

A professional penetration tester will have knowledge of the system being tested and a greater understanding of the context in which the system operates, ensuring the test simulation comes very close to replicating a real malicious attack.

3. Produce scope statements

Your penetration testing programme should include formal scope statements for penetration testing, supported by defined reporting requirements, prior to tests commencing. Arrangements should be made to ensure your service provider(s) will meet your requirements.

The scope of penetration tests should be recorded in a formal document signed-off by all relevant parties. It should include a definition of the target environment, specify resourcing requirements, define liabilities, authorise testing to be conducted and include follow-up activities.

Relevant parties (ie. named individuals or groups) required to sign-off the scope statement should include authorised and suitably qualified individuals from all relevant parties plus relevant and qualified individuals, dependent on the value of the system being tested (or similar).

The table right outlines elements typically included in a scope statement. This information will need to be disseminated throughout the organisation, for example to operations staff that may mistakenly report testing activities as actual attacks on the organisation.

Scoping element	Considerations
Definition of target environment	– Which systems are in and out of scope – The testing approach being adopted (e.g. Black-, white- or gray-box) – Types of tests that are prohibited (e.g. 'denial of service' type testing) – Where the testing team will need to be to conduct the testing (e.g. on the customer's site or at the test supplier's premises) – Approvals required for the testing to go ahead
Network or web application firewalls deployed	– Who will be leading the testing engagement – The names of testers that will be used for the testing engagement, with details about their roles, skills, experience, qualifications and backgrounds – The number of days required – and the days when testing will take place – Defined testing times and locations
Report requirements	– The format of the test report (template often used) – When the test report will be delivered (not later than a few days after completion of the test) – How the test report will be delivered (electronic and / or physical)
Communication processes	– Information and resources that the testers will need prior to testing – How affected third parties will be informed and consulted in relation to testing activities – How testing start-up and close-down will be covered – Regular (often daily) communications (e.g. teleconferences or meetings) – Approvals required for various elements of the testing that will be going ahead
Liabilities of both parties	– Steps required by both parties should problems (e.g. slippage) arise – Details of liability (indemnity) insurance held by the testing supplier
Follow-up activities	– Presentation of key findings and recommendations to senior management – Any re-testing needed once mitigations have been made for the discovered vulnerabilities required by both parties should problems (e.g. slippage) arise

The penetration tester must be authorised to perform any tests on your systems, which can often be achieved by formally defining what is to be tested and how it will be tested. The test team will also require a disclaimer stating it is legally authorised to carry out specified activity on your property and systems.

Reporting formats

Effective reporting is a critical aspect of penetration testing, yet its importance is often overlooked. The format and content of reporting should be defined in both the scope and in a formal contract.

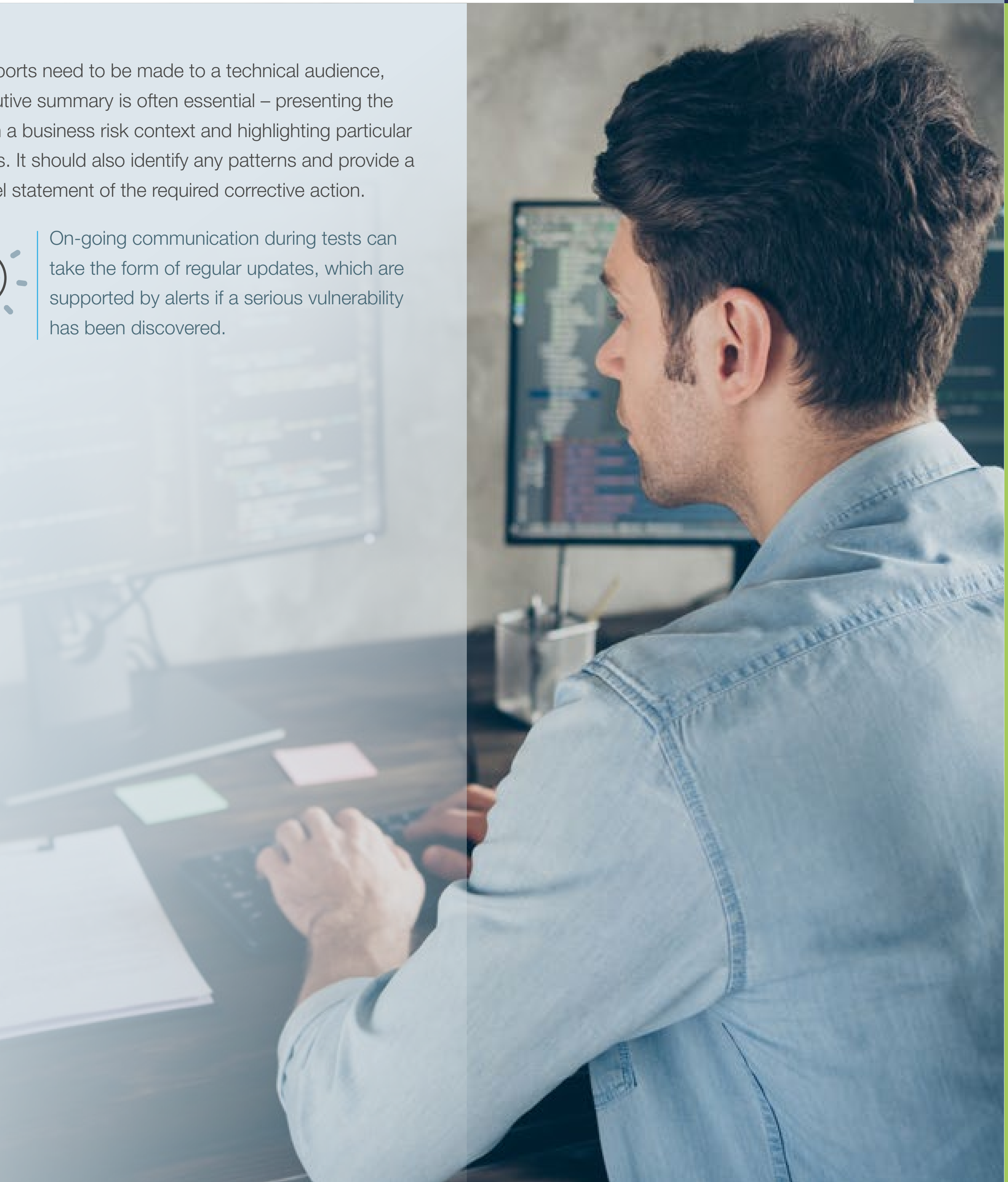
Depending on test objectives, you should ensure your service provider will:

- Provide a detailed technical report on the vulnerabilities of the system
- Explain the vulnerabilities in layman's terms for senior management
- Report the outcome of the test in business risk terms
- Identify short term (tactical) recommendations
- Conclude with and define 'root cause' long term (strategic) recommendations
- Include a security improvement action plan
- Provide assistance in implementing the security improvements

A good report will include the names, roles and qualifications of the testers, date of the report, type of test undertaken and test scope. It should highlight any issues affecting the validity of the results and any other unknowns or anomalies encountered during testing.

While reports need to be made to a technical audience, an executive summary is often essential – presenting the results in a business risk context and highlighting particular concerns. It should also identify any patterns and provide a high-level statement of the required corrective action.

On-going communication during tests can take the form of regular updates, which are supported by alerts if a serious vulnerability has been discovered.



4. Establish a management assurance framework

Once scope is defined, some organisations leave the supplier to conduct penetration testing with little further interaction. However, this may not result in optimum or desired results being obtained. It can also lead to significant difficulties if problems arise, either with the test itself or the way the test is conducted.

Consequently, your penetration testing programme should include creating a documented management assurance framework to help govern all aspects of penetration tests, ensuring that testing scope is documented in a comprehensive agreement and that testing meets requirements.

An effective management assurance framework will establish control processes over all important management aspects of testing, such as:

- Test administration (e.g. scope, legal constraints, disclosure, and reporting)
- Test execution (e.g. approach, separation of systems and duties, tool heritage, traceability and repeatability of tests)
- Data security (e.g. secure storage, transmission, processing and destruction of critical or sensitive information provided or accessed during the test, test results and recommended actions)

All aspects of penetration testing need to be managed effectively, for example by:

- Establishing an assurance process to oversee the testing
- Monitoring performance against requirements
- Ensuring appropriate actions are being taken

Ideally, you, as the client, should establish and control the management assurance framework. Your supplier should be aware of these needs and help you define and adhere to your management assurance framework. But responsibility for the actual systems and data – and any assurance about them – rests with your organisation.

Contract definition

It is important that the test's scope is clearly defined in a legally binding contact, signed off by all relevant parties before testing starts.

The contract should be referred to a legal team to ensure terms of business and detail of the contract and schedule of work are acceptable, as suppliers often:

- Caveat risks to your organisation (and theirs)
- Require you to acknowledge that you understand penetration testing involves an element of risk
- Seek indemnities from you for work that they undertake

As well as the scope of the testing to be undertaken, the contract should also include:

- Explicit exclusions (e.g. systems that are out of scope)
- Technical and operational constraints
- Roles and responsibilities for all parties concerned
- Specific legal and regulatory requirements
- Timings and checkpoints
- A problem escalation process
- Reporting and presentation style
- Post-test corrective action strategy and action plan development
- Pricing and terms of business

You should consider requiring your supplier to:

- Nominate a senior manager (who can be easily contacted during the testing process) to be accountable for managing test delivery
- Clearly explain the limits and dangers of the security test as part of the statement of work
- Provide confidentiality and non-disclosure of customer information and test results

5. Implement management control processes

Your penetration testing programme should include implementing effective risk, change and problem management processes that apply to all aspects of penetration testing.

Methods of keeping risks to a minimum include:

- Carrying out planning in advance
- Having a clear definition of scope
- Using predefined escalation procedures, and
- Using individual testers with relevant experience and qualifications that work for certified organisations

An effective change management process should:

- Cover changes to the scope of the penetration test, organisational controls and individuals on the testing team
- Ensure all parties involved adhere to the process, and
- Ensure changes to penetration testing are made quickly and efficiently

An effective problem management process should cover tests not working as planned, problems caused as a result of the penetration testing, breaches of contract or codes of conduct and effective, timely problem resolution.

Risk mitigation

Your organisation needs to be aware that performing any sort of penetration test carries some risk to the target system and business information associated with it (e.g. degradation or loss of services and disclosure of sensitive information).

You should develop methods of keeping risks to your organisation to a minimum during penetration testing in a variety of ways, which include:

- Carrying out planning in advance
- Clear definition of scope
- Predefined escalation procedures

When conducting penetration tests, you should ensure those responsible for running the target systems:

- Have full knowledge of the tests to help protect against unexpected business consequences, such as an inadvertent trigger of internal controls
- Are aware of, and adhere to, any escalation procedures

You should ensure those responsible for running target systems are available during the test period to help:

- Ensure testing takes place as agreed
- Keep risks within acceptable boundaries
- Deal with any problems
- Manage issues that have been escalated

Risks associated with penetration testing can be reduced if the business utilises a qualified and experienced penetration tester (CREST certified), working within the structured constraints of a certified testing company such as a CREST member.

Change management

Any changes to the scope of the penetration test (e.g. additional testing requested, such as wireless or device testing) or to organisational controls (e.g. to address a critical weakness uncovered during testing) need to be managed quickly and efficiently. Consequently, a change management system should be applied to any changes in the testing scope or configuration of target systems.

Your change management process should cover changes to:

- The scope of the penetration test
- Organisational controls
- The individuals on the testing team

You should ensure all parties involved, including suppliers and other third parties, adhere to your change management process.

Problem resolution

Problems (and complaints) can arise during the test, for example, due to resources not being made available, tests not working as planned or a breach of a code of conduct. It is important to ensure there is a problem resolution process in place, so any problems arising during penetration testing are resolved in an effective and timely manner, in accordance with your problem management process.

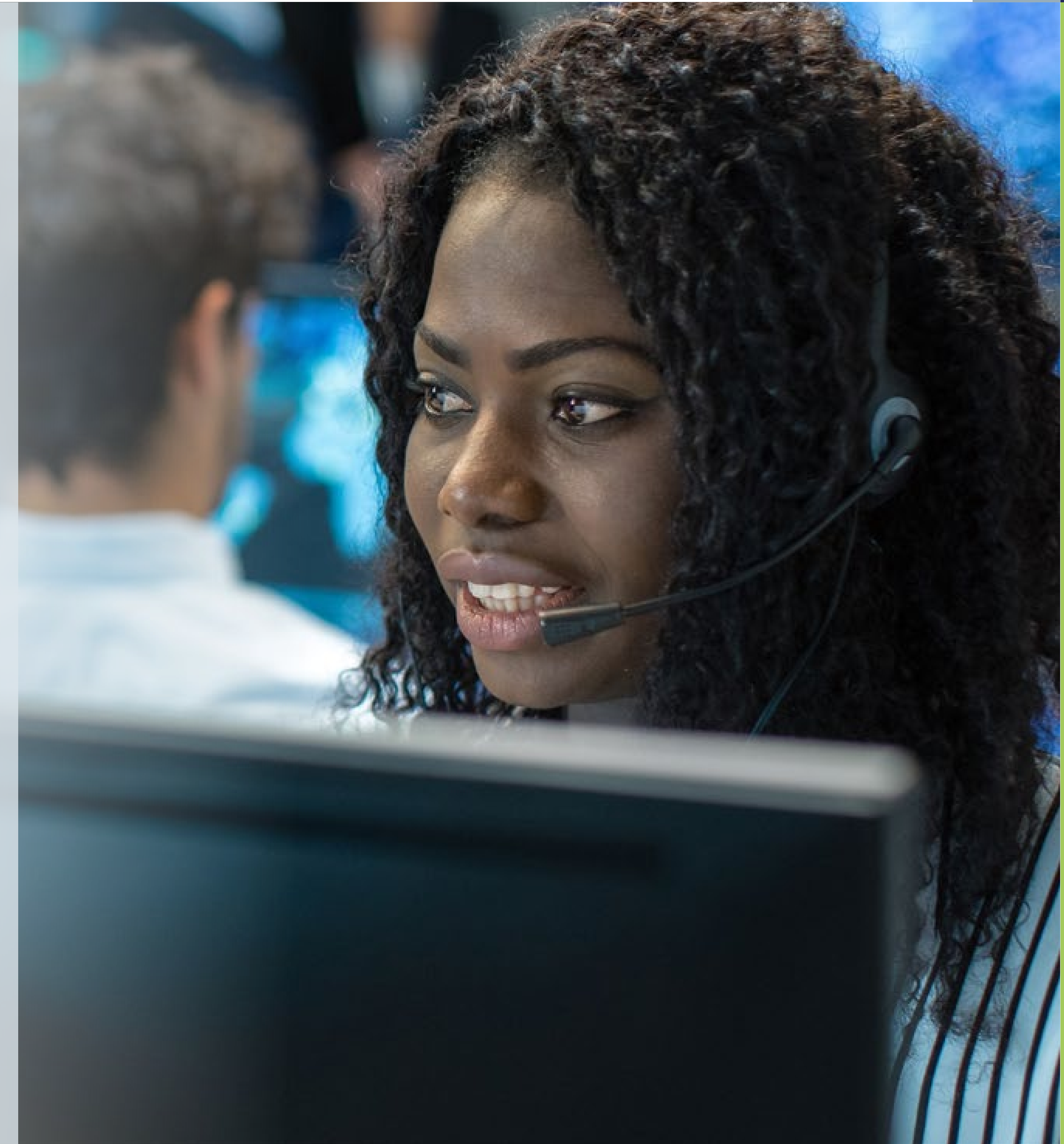
Your problem resolution process should cover tests not working as planned and resources not being made available. It should also cover problems caused as a result of the penetration testing, which may include:

- Interruptions to, or degradation of, live systems
- Unauthorised disclosure of confidential information
- Compromise of the integrity of information (e.g. affecting the accuracy or timeliness of information)

Your problem resolution process should include:

- Breaches of contract
- Specifications in the scope statement
- A relevant code of conduct

CREST members – and the penetration testers they employ – are required to adhere to rigorous codes of conduct for both the individual testers and organisations they work for, backed up by an independent investigation scheme should conflicts arise. Details of these codes are available from CREST **here**.



6. Use an effective testing methodology

Your penetration testing programme should specify that, when conducting penetration tests, organisations should use a systematic, structured testing methodology.

Broadly, all forms of penetration testing adhere to some variant of the process shown in Figure 9 below, and tests should progress through each of these steps in order. The activities performed and amount of time spent on each step will vary depending on the nature of the test, the scope agreed prior to testing, and the target system.

A systematic, structured testing methodology should:

- Be based on proven approaches
- Align with authoritative publicly available sources
- Detail specific evaluation or testing criteria
- Adhere to a standard common language and scope for performing penetration testing, and
- Specify a required approach (or approaches) for carrying out all stages of a comprehensive end-to-end penetration test

Your service providers should demonstrate compliance with 'standard' methodologies, if required, and develop or augment the testing methodologies that each scenario demands.

Authoritative publicly available sources for standard penetration testing methodologies are available, which apply to:

- Infrastructure testing, such as the **Open Source Security Testing Methodology Manual (OSSTM)** and **Penetration testing in SP800-115[3]** and the **Open Web Application Security Project® (OWASP)**
- Web application testing, such as OWASP

Your penetration testing methodology should:

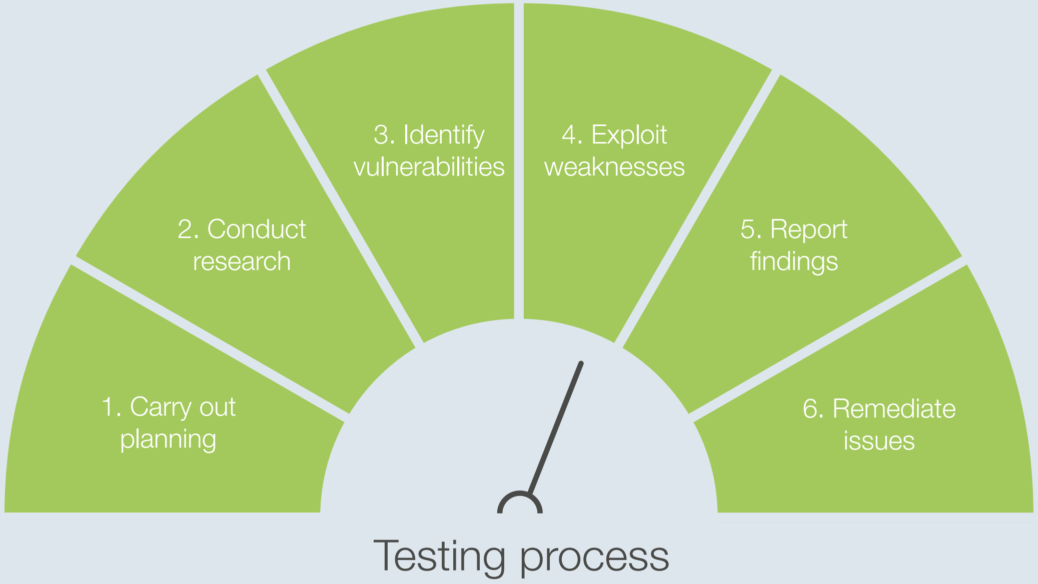
- Detail specific evaluation or testing criteria
- Adhere to a standard common language and scope for performing penetration testing (i.e. security evaluations), such as the **Penetration Testing Execution Standard (PTES)**

The main publicly available methodologies are outlined in the box on the following page, entitled *Penetration testing initiatives*.

Leading suppliers are fully aware of all the main methodologies, but often feel they are not comprehensive enough. Consequently, most suppliers have developed their own methodologies, but are able to show compliance to other 'standard' methodologies if required.

Any methodology should merely be a guideline. The actual testers often spend considerable time trying to hack into a system using any method they can, and the good ones develop the most appropriate (informal) methodology that each scenario demands.

Figure 9: The service provider selection process



Penetration testing initiatives

There are several penetration testing initiatives being produced by collaborative (often open or free source) bodies. These initiatives include security assessment frameworks or standards, testing processes, structures or approaches and useful sources of information about testing techniques and common vulnerabilities. Some of the main penetration testing initiatives are summarised below.

OSSTM

The Open Source Security Testing Methodology Manual (OSSTMM) is a peer-reviewed methodology for performing security tests and using metrics. The OSSTMM focuses on the technical details of exactly which items need to be tested, what to do before, during, and after a security test and how to measure the results. OSSTMM is also known for its Rules of Engagement that define, (for both tester and client) how the test needs to properly run, starting from denying false advertising from testers to how the client can expect to receive the report. New tests for international best practices, laws, regulations, and ethical concerns are regularly added and updated.

OWASP

The Open Web Application Security Project® (OWASP) is an open community dedicated to enabling organisations to develop, purchase and maintain applications that can be trusted. All OWASP tools, documents, forums and chapters are free and open to anyone interested in improving application security. It advocates approaching application security as a people, process and technology (PPT) problem because the most effective approaches to application security include improvements in all of these areas.

NIST

The National Institute of Standards and Technology (NIST) mentions penetration testing in SP800-115[3]. NIST's methodology is less comprehensive than the OSSTMM. However, it is more likely to be accepted by regulatory agencies. For this reason, NIST refers to the OSSTMM.

PTES

The Penetration Testing Execution Standard (PTES) is an emerging standard being produced by a reputable group of volunteer penetration testing specialists. It is designed to provide both businesses and security service providers with a common language and scope for performing penetration testing (i.e. security evaluations).

7. Conduct sufficient research and planning

Your penetration testing programme should include producing detailed test plans to provide guidelines for the penetration testing, including imitating research activities a potential attacker could undertake to find out as much about the target environment as possible.

Carry out planning

Detailed, agreed test plans should be produced to provide guidelines for penetration testing. It should specify what will actually be done during the test and should be agreed by all relevant parties.

“A good test plan helps to assure the process for a proper security test without creating misunderstandings, misconceptions or false expectations”.

A detailed test plan should be produced by your testing service provider that:

- Specifies what will be done during tests – often a series of discrete tasks
- Provides a mechanism for formally agreeing testing scope and all testing activities so both parties can ensure their needs are met and terms of reference for testing activities are clear
- Is flexible enough to accommodate changes in test priorities, while not impeding on actual testing time

Test plans should be agreed with your organisation prior to any testing commencing.

Conduct research

Penetration tests should include sufficient research to imitate research activities a potential attacker could undertake to find out about the target environment and how it works.

Research undertaken should include gathering, collating and analysing relevant information about the target environment. Typical techniques are described in the table below.

Technique	Description
Information gathering	Collating and analysing information about the target, often available: – From public sources of information, including the Internet. – Through information sharing networks (e.g. CERTs) – Via authorised social engineering sources – Based on threat intelligence This can provide considerable detail about an organisation, including its technology environment, type of business and security structure.
Reconnaissance	Obtaining positive confirmation of information about the target. Contact is made with the organisation to confirm that system configuration and security controls are as expected. Examples include: visiting a target site as a guest or bystander to confirm physical details and sending traffic to confirm the existence of routers, web servers and email servers.
Network enumeration / scanning	Establishing potential access points offered by a target. In a network test, this can involve scanning for open services on targets, or establishing the existence of possible user identification credentials.
Discovery and assessment	Learning about a target’s infrastructure (by ‘foot printing’, mining blogs, or using search engines and social networking sites) and determining how the target system works.

8. Identify and exploit vulnerabilities

Your programme should specify that penetration testers must identify a range of potential vulnerabilities in target systems, then try to exploit those vulnerabilities and penetrate the target system, in a controlled manner.

Vulnerability identification and exploitation typically include testers examining technical system, network and application vulnerabilities and security control weaknesses. This will be supported by a range of techniques, (including exploit, escalation, advancement and analysis techniques) to try and take advantage of specific weaknesses.

Identify vulnerabilities

The objective is to identify a range of potential vulnerabilities in a target system, which will involve the tester examining:

- Attack avenues, vectors and threat agents, using attack trees for example
- Results from threat analysis
- Technical system, network and application vulnerabilities

The types of testing should include automated attack methodologies (scanning), manual testing (experimenting with numerous tools) and additional techniques (such as artificial intelligence, enabling more iterations of an attack to be performed.

Tests should include:

- Reviewing vulnerabilities identified by third parties, such as the '**OWASP Top Ten**', which presents a list of common security vulnerabilities found in web applications (injection attacks, cross-site scripting and failure to restrict URL access)
- Identifying the cause of any vulnerability discovered, for example a vulnerability resulting from a lack of understanding of IT security issues (by web developers and users of mobile devices, for example)

Exploit weaknesses

Once vulnerabilities have been identified in the target environment, testers should use exploitation frameworks, stand-alone exploits, and other tactics to try and take advantage of these weaknesses – using precision strikes or customised exploitation, for example – to penetrate the target system.

Testers will use a range of techniques to try and take advantage of specific weaknesses, including:

Technique	Description
Exploit	Using identified vulnerabilities to gain unauthorise access to the target. For example, in a web application test, this may involve injecting commands into the application that provide a level of control over the target. Exploitation may require combining several sets of information in a creative way.
Escalation	Gaining further access within a target, once an initial level of access has been obtained. For example, in a network test, successful exploitation may allow user or guest access to a system. Escalation through additional exploitation will typically be required to obtain administrative privilege.
Advancement	Attempting to move on from the compromised target to find other vulnerable systems. For example, in a network test this will consist of "hopping" from one system to another, potentially using the access obtained on the original target to access other systems. In a physical test, this might involve moving from one compromised building to another.
Analysis	Analysing and verifying raw data to ensure testing is thorough and comprehensive. Depending upon the environment, consultants may conduct additional manual tests. They will then interpret the results to produce a tailored, business-focused report.

9. Report key findings

Your programme should specify that key findings identified during penetration tests should be formally presented to your organisation by suppliers. The pen testers should provide details such as how they found the vulnerabilities; what the outcome of exploiting each vulnerability could be; the level of business risk for each vulnerability and advice on how to remediate each vulnerability.

Outputs from testing, where required, should be stored safely and securely deleted.

Findings identified during the penetration test should be recorded in an agreed format, describing each finding in:

- Technical terms that can be acted upon
- A non-technical, business context, so justifications for corrective actions are understood
- A formal, well-designed testing report

Reports should describe the vulnerabilities found, including:

- Test narrative – describing the process that the tester used to achieve particular results
- Test evidence – results of automated testing tools and screen shots of successful exploits
- Details about the associated technical risks – and how to address them

Penetration testing reports should be used to present remediation activities undertaken and the root causes of issues identified. These reports should be:

- Disseminated to relevant stakeholders
- Supported by debriefing sessions
- Acted upon

It is often helpful to ensure suppliers use a common reporting template, enabling results comparison between different tests and providers.

Once the report has been digested and notes taken, a presentation should be arranged with your supplier for them to present the key findings, highlighting:

- How they found the vulnerabilities
- What the outcome of each vulnerability could be
- The level of business risk
- Details of who else should be informed – such regulators or law enforcement
- Remediation advice

Stakeholders in your organisation should:

- Understand penetration testing reports
- Take appropriate action to address issues

The outputs from penetration tests should be fed in to your:

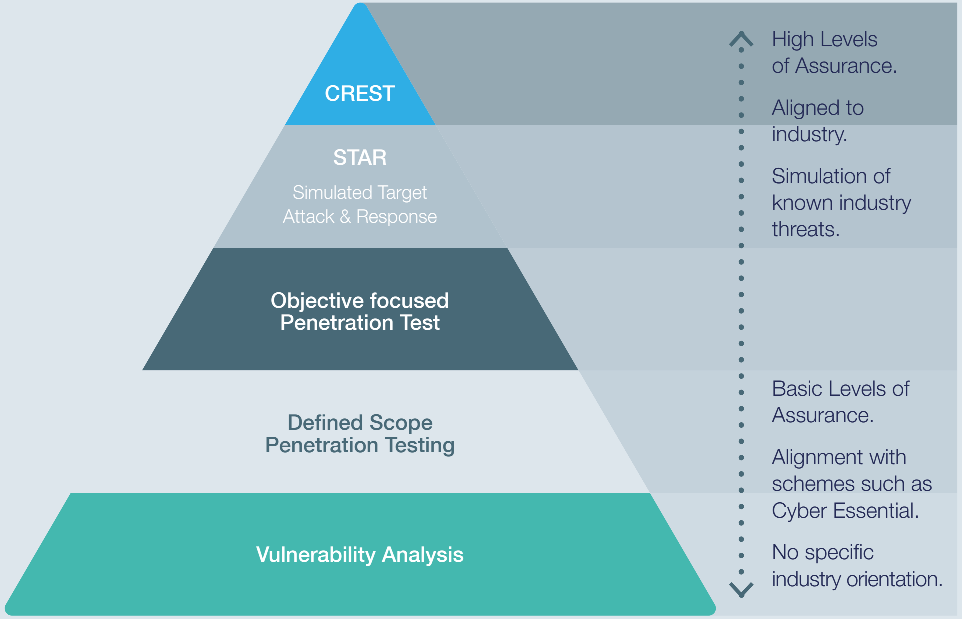
- Incident response processes
- Risk management processes
- Technical security monitoring services, such as in a Security Operations Center (SOC)
- Technical security tool configurations (eg. IDS, IPS, and DLP)

Penetration testing should include:

- Reporting to senior management through schemes such as CBEST in the financial services sector and TBEST in the telecom sector
- Any requirements to report to a regulator or government body

CREST develops and supports a range of outcome-based technical assurance schemes, ranging from regulatory-based testing, through industry-led assurance testing for certain industries, to intelligence-led penetration testing through schemes like STAR, CBEST and TBEST. A summary of the different levels of technical assurance available is shown in Figure 10 below.

Figure 10: Technical security assurance schemes

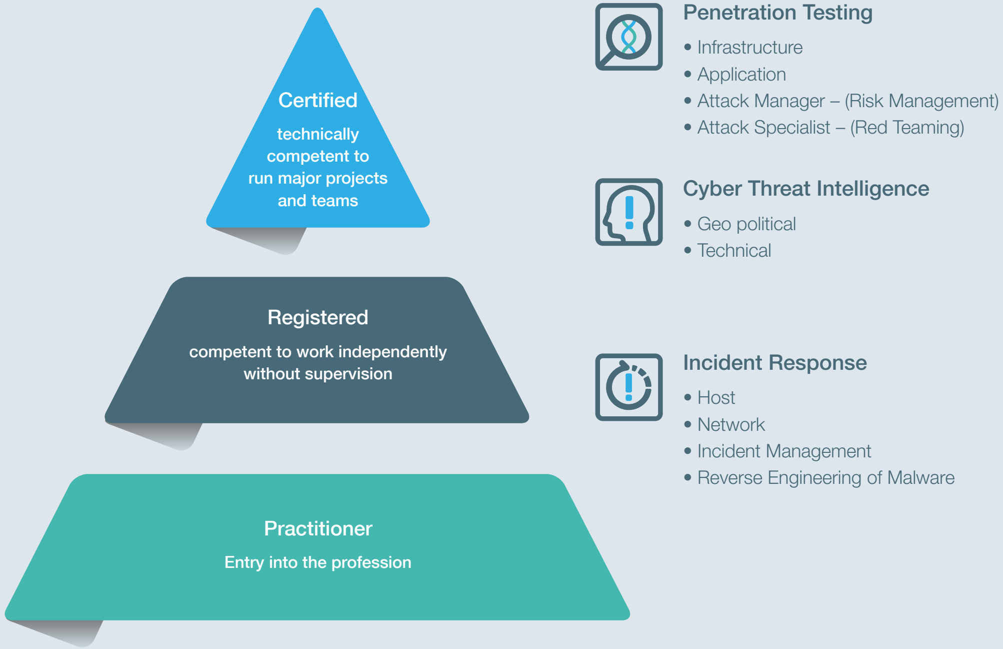

CREST
STAR
Simulated Target Attack & Response
Objective focused Penetration Test
Defined Scope Penetration Testing
Vulnerability Analysis
High Levels of Assurance.
Aligned to industry.
Simulation of known industry threats.
Basic Levels of Assurance.
Alignment with schemes such as Cyber Essential.
No specific industry orientation.

CREST's offerings differ from other security testing because they are threat intelligence based, less constrained and focus on the more sophisticated and persistent attacks against critical systems and essential services. The inclusion of specific threat intelligence ensures tests replicate the evolving threat landscape as closely as possible, so remain relevant.

Many CREST members have been accredited by the Bank of England to deliver CBEST penetration testing using the already stringent standards for assessing the capabilities, policies and procedures that CREST member companies have to achieve. CBEST accredited professionals also need to demonstrate extremely high levels of technical knowledge, skill and competency.

CREST also develops and supports a series of professional qualifications in technical security including penetration testing, threat intelligence and incident response. A summary of the different levels of examination provided is shown in Figure 11 below.

Figure 11: Examinations supporting professional qualifications in technical security testing


Certified
technically competent to run major projects and teams
Registered
competent to work independently without supervision
Practitioner
Entry into the profession
Penetration Testing
• Infrastructure
• Application
• Attack Manager – (Risk Management)
• Attack Specialist – (Red Teaming)
Cyber Threat Intelligence
• Geo political
• Technical
Incident Response
• Host
• Network
• Incident Management
• Reverse Engineering of Malware

Details of the CREST approved threat intelligence service suppliers and penetration testing companies can be **found here**. These organisations are CREST STAR members, to allow the scheme to be extended beyond financial services to other parts of critical national infrastructure.

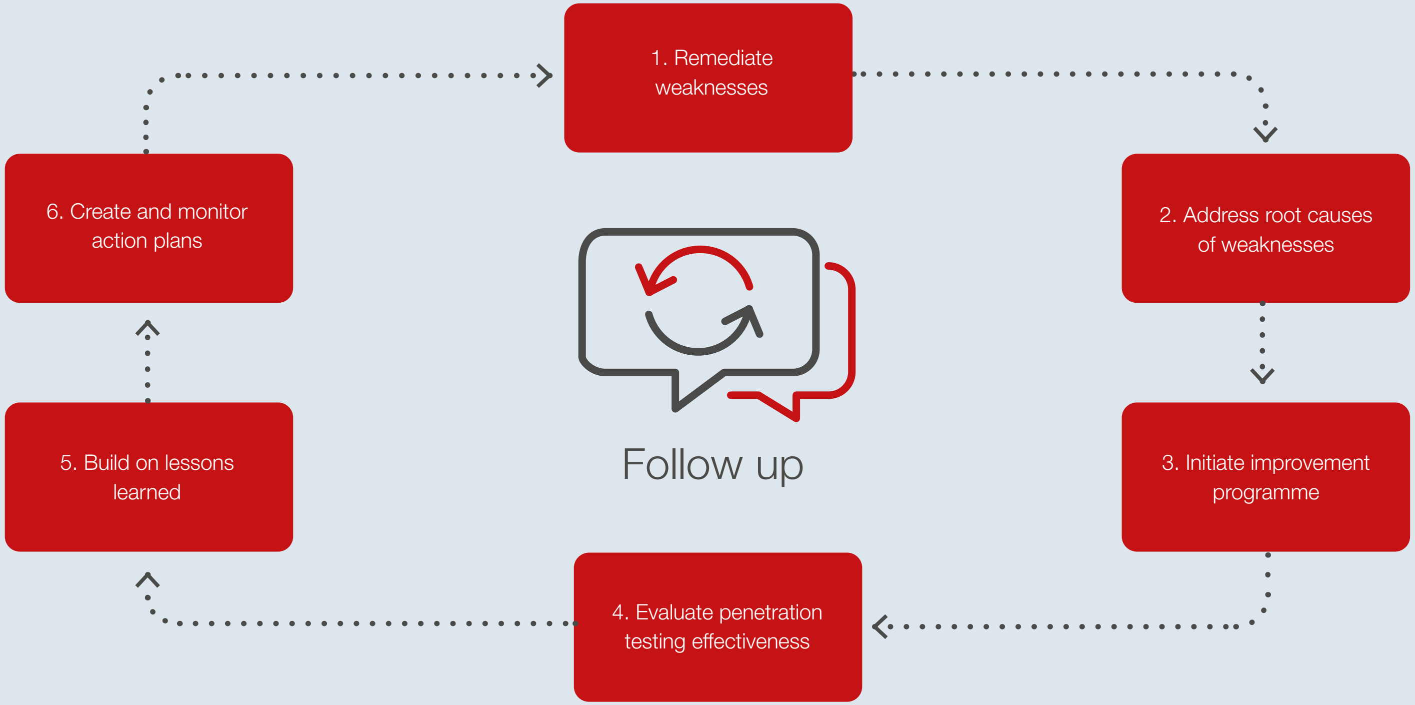
Part 5 – Follow up

Overview

Once each penetration test is complete – and any identified vulnerabilities addressed – it can be tempting to draw a line under the process and return to business as usual. However, to reduce risks in the longer term and across the whole organisation, it is useful to carry out a range of follow up activities, which include initiating an improvement programme.

Steps following each individual penetration test performed as part of the enterprise-wide penetration testing programme are outlined in Figure 12 below.

Figure 12: The follow up process



1. Remediate weaknesses
2. Address root causes of weaknesses
3. Initiate improvement programme
4. Evaluate penetration testing effectiveness
5. Build on lessons learned
6. Create and monitor action plans
Follow up

These six actions are described on the following pages.

1. Remediate weaknesses

Your penetration testing programme should specify follow-up activities include remediating weaknesses found during the testing process, in line with a comprehensive and approved remediation process solution, to reduce the risk of them being exploited again.

The remediation process should be carried out by appropriately qualified, experienced technical security professionals, and include:

- Addressing all issues raised in penetration testing reports
- Applying immediate or short term solutions, such as patching systems, closing ports and preventing traffic from particular web sites or IP addresses
- Replicating results of penetration tests, using technical data, for example
- Determining which weaknesses to address first. This could be based on risk ratings for critical asset, for example
- Reporting weaknesses to relevant third party organisations (CERTs, BUGTRAQ, etc)
- Feeding these remediation actions into longer term solutions, such as an updated patch management strategy or a whitelisting / blacklisting policy
- Agreeing short-term re-testing or verification activities

2. Address root causes of weaknesses

Your penetration testing programme should specify that follow-up activities include analysing and addressing the root causes of weaknesses identified during penetration testing.

Root cause analysis should include:

- Identifying the real root causes of exposures – not just the symptoms of an attack
- Evaluating the potential impact of exposures on the business
- Identifying more endemic or fundamental root causes
- Involving qualified, experienced security professionals to help define corrective action strategy and plans

3. Initiate improvement programme

Your penetration testing programme should specify that, on completion of penetration tests, an improvement programme should be initiated.

The improvement programme should be carried out in a structured, systematic manner:

- Addressing root causes of weakness
- Evaluating penetration testing effectiveness
- Identifying lessons learned and applying good practice enterprise-wide
- Creating and monitoring action plans
- Agreeing approaches for future testing

4. Evaluate penetration testing effectiveness

The effectiveness of your penetration tests should be evaluated. This evaluation should include:

- Determining if objectives were met
- Assessing if sufficient weaknesses were identified, and in a sensible timeframe
- Reviewing exploitations undertaken, on a sample basis
- Comparing test results to external benchmarks

The effectiveness of your penetration testing programme should be evaluated, including:

- Benchmarking the testing programme against other similar organisations (of a comparable size, sector and region)
- Determining if value for money is being obtained from your service providers

5. Build on lessons learned

Follow-up activities can include identifying, recording, analysing and acting upon lessons learned, ensuring good practices are applied to other environments.

Lessons learned before, during and after penetration tests have been conducted should be used to:

- Determine the effectiveness of previous remediation activities
- Plan for future tests
- Provide feedback to service providers to help them improve processes

Good practices (including fixes) identified as a result of penetration tests conducted for one environment should be applied to a range of other environments and rolled out in a consistent, effective manner, fixing root causes.

Lessons learned should be used to help improve ground up, end-to-end security, develop an integrated security programme and support:

- Reactive learning (to help understand technical security practices and act upon penetration testing results)
- Proactive learning (to help stop vulnerabilities arising in the future or being further exploited)

6. Create and monitor action plans

Action plans help act upon follow-up activities undertaken and provide input into the design and scope of future tests. They should be formally documented, formulated by competent technical experts, reviewed by business management and signed-off by senior management.

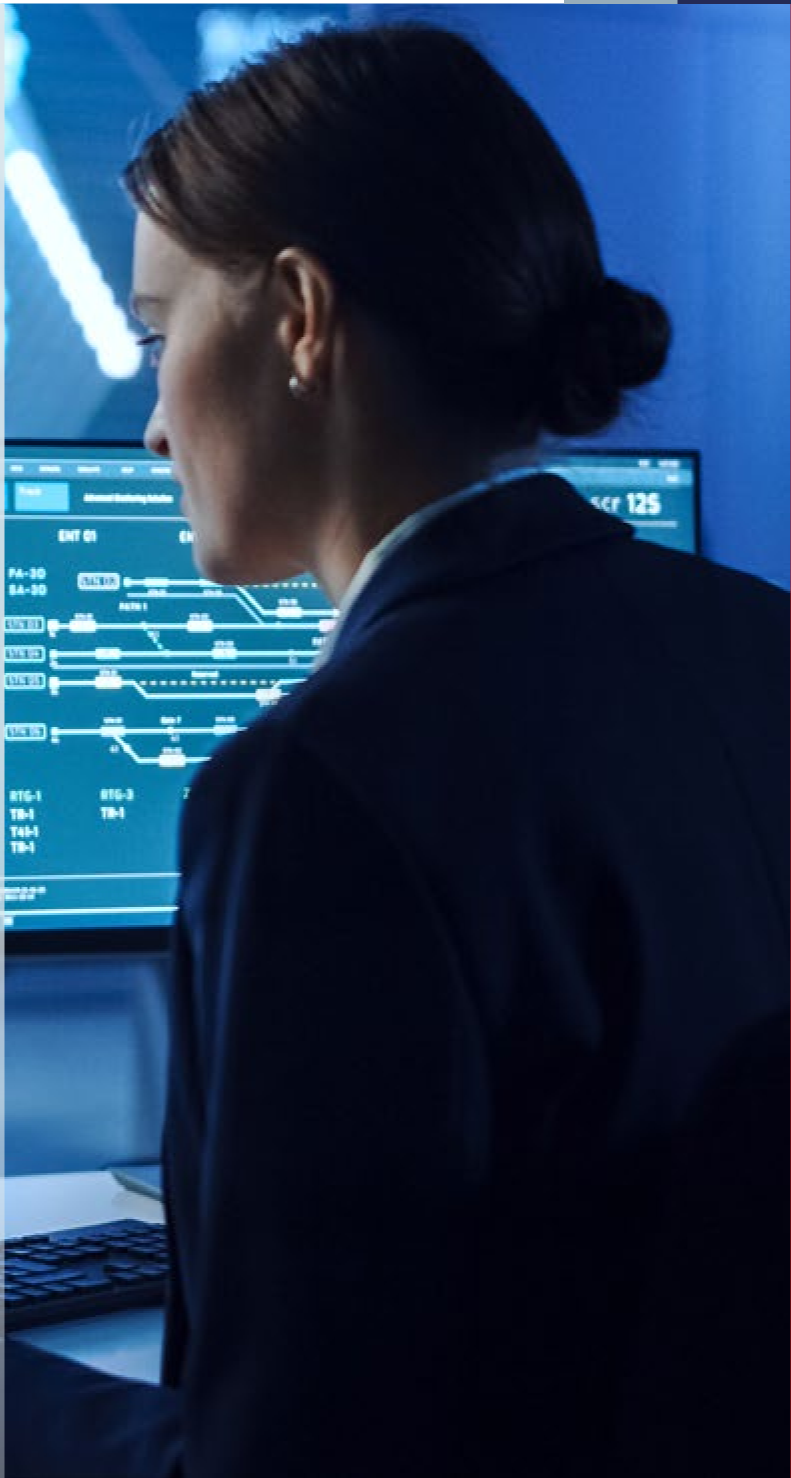
Action plans should:

- Outline all the relevant actions to be taken to prevent vulnerabilities identified through testing from recurring
- Help improve the overall information security programme
- Include a brief description of each action, including their priority and category, individuals responsible and accountable for each action and target dates for completion

Action plans should be implemented effectively within critical timescales and then monitored on a regular basis to:

- Ensure progress is being made
- Highlight any delays or difficulties being experienced
- Reassess the level of risk

- What to test in the future (infrastructure, web applications, mobile devices, wireless systems or industrial control systems)
- How future tests should be undertaken (white, gray or black-box testing; internal or external testing)
- When tests should be undertaken in the future, after significant technical or business changes are made or in response to a major security incident, for example



Part 6 – Penetration testing maturity assessment

Maturity model

To carry out penetration testing effectively, you need to build an appropriate penetration testing programme, the maturity of which can be assessed against a suitable maturity model by using the CREST suite of penetration testing maturity assessment tools.

One of the best ways to determine effectiveness is to measure the level of maturity of your penetration testing programme in terms of:

- People, process, technology and information
- Preparation, testing and follow up

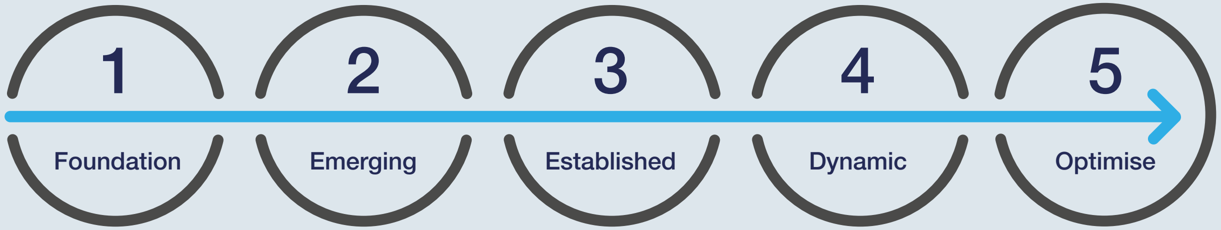
The maturity model used in the CREST penetration testing maturity assessment tools is based on a traditional, proven model shown below. This model can be used to determine the level of maturity of your penetration testing programme, ranging from 1 (least effective) to 5 (most effective), as shown in Figure 13 below.

Different types of organisation require different levels of maturity for their penetration testing programmes. For example, a small company operating in the retail business will not have the same requirement – or ability – to carry out penetration tests in the same way as a major corporate organisation in the finance sector – or a government department.

Consequently, the level of pen test programme maturity should be reviewed in context and compared to your actual requirements. Your organisation can then be compared with similar organisations to help determine if the level of maturity is appropriate.

The maturity of your penetration testing programme can play a significant role in determining the level of third-party involvement required to conduct independent penetration testing. Organisations with a mature penetration testing programme may manage most of their operations in-house, while those who are less mature may depend entirely on third parties.

Figure 13: The Penetration Testing Programme maturity model



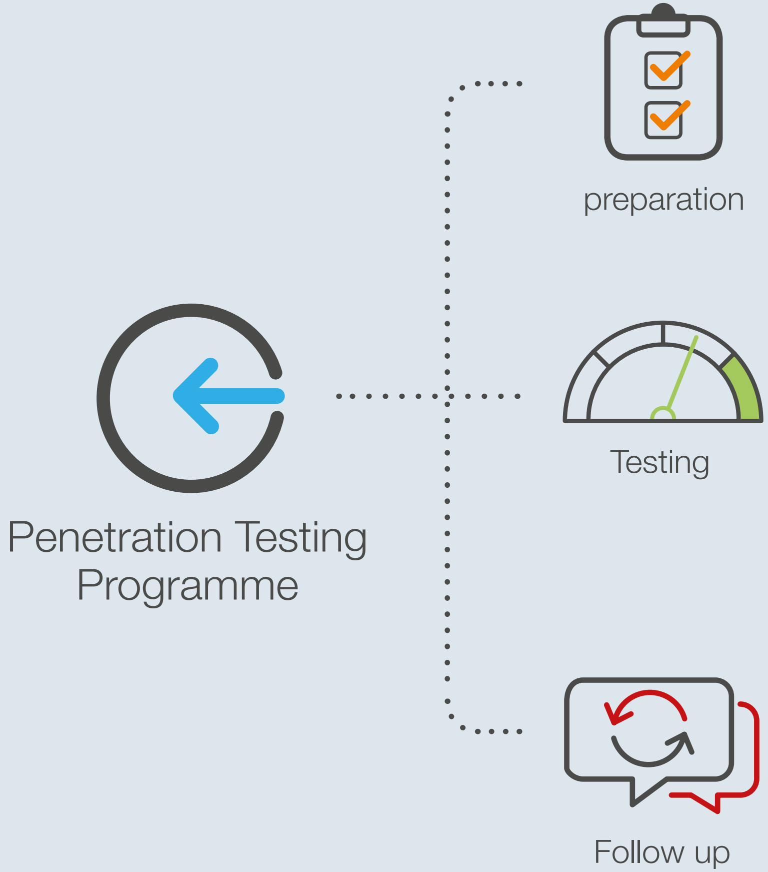
Maturity assessment

The effectiveness of your programme should be evaluated regularly against approved criteria to help determine if objectives were met and value for money has been obtained from your supplier(s).

CREST penetration testing maturity assessment tools have been developed in conjunction with representatives from a broad range of organisations, including industry bodies, consumer organisations, the UK government and suppliers of expert technical security services.

You can assess the status of your penetration testing programme on the industry standard scale of 1 (least effective) to 5 (most effective) for each of the 22 steps in the 3 stages of the CREST penetration testing programme outlined in Figure 14, right.

Figure 14: The Penetration Testing Programme



preparation:

1. Maintain a technical security assurance framework
2. Establish a penetration testing governance structure
3. Evaluate drivers for conducting penetration tests
4. Identify target environments
5. Define the purpose of the penetration tests
6. Produce requirements specifications
7. Select suitable suppliers

Testing:

1. Agree testing style and type
2. Identify testing constraints
3. Produce scope statements
4. Establish a management assurance framework
5. Implement management control processes
6. Use an effective testing methodology
7. Conduct sufficient research and planning
8. Identify and exploit vulnerabilities
9. Report key findings

Follow up:

1. Remediate weaknesses
2. Address root causes of weaknesses
3. Initiate improvement programme
4. Evaluate penetration testing effectiveness
5. Build on lessons learned
6. Create and monitor action plans

The maturity assessment tools

The CREST penetration testing maturity assessment suite comprises three spreadsheet-based tools:

- A Summary assessment tool (no macros), which allows an assessment to be made to determine the level of maturity of your penetration testing programme at a high level
- An Intermediate assessment tool (no macros), which allows an assessment to be made at an intermediate, more detailed level
- A Consolidated assessment tool (requires macros to be enabled), which allows more sophisticated assessments to be made to determine the level of maturity of your penetration testing programme at summary, intermediate or detailed levels – or a combination of all three

Each assessment tool comprises a set of worksheets, enabling assessment to be made in a consistent manner at either summary, intermediate or detailed level.

The summary version allows a quick, high-level overview to be obtained. The detailed tools enable more precise assessment of the maturity level of your penetration testing programme. The results presented in all the tools are based on responses given to a series of well-researched questions that have been validated by industry experts. You can select relevant responses to each question in the Assessment worksheets.

The penetration testing maturity assessment tools form part of a series of assessment tools developed by CREST, including high level and detailed *Cyber Security Incident Response Maturity Assessment* Tools.

Based on your responses to the questions in the Assessment worksheets, your level of maturity for each of the 22 steps is calculated using an algorithm that takes account of both the level of response to each question and the associated weighting factor.

The results derived from completion of the Assessment worksheets are automatically:

- Shown as ratings for individual questions and aggregated up to action level, area level or for the entire penetration testing capability
- Presented in graphical format against the organisation's target profile, either as a bar chart or radar diagram
- Highlighted in a heat map using a traffic light system to highlight results as red, amber or green against user-defined ranges

A useful results summary is presented as a bar chart in the Results worksheet, as shown in the example at Figure 15. These results show the level of maturity for your penetration testing programme on a scale of 1 to 5, previously described, comparing this to user configurable maturity ratings, based on your chosen target profile and benchmark ratings.

You can assign a benchmark rating by simply overwriting the relevant figure in the right-hand Benchmarking Rating column. This is not automatically calculated or imported, so needs to be based on benchmark analysis performed independently either by your own organisation or an external service provider.

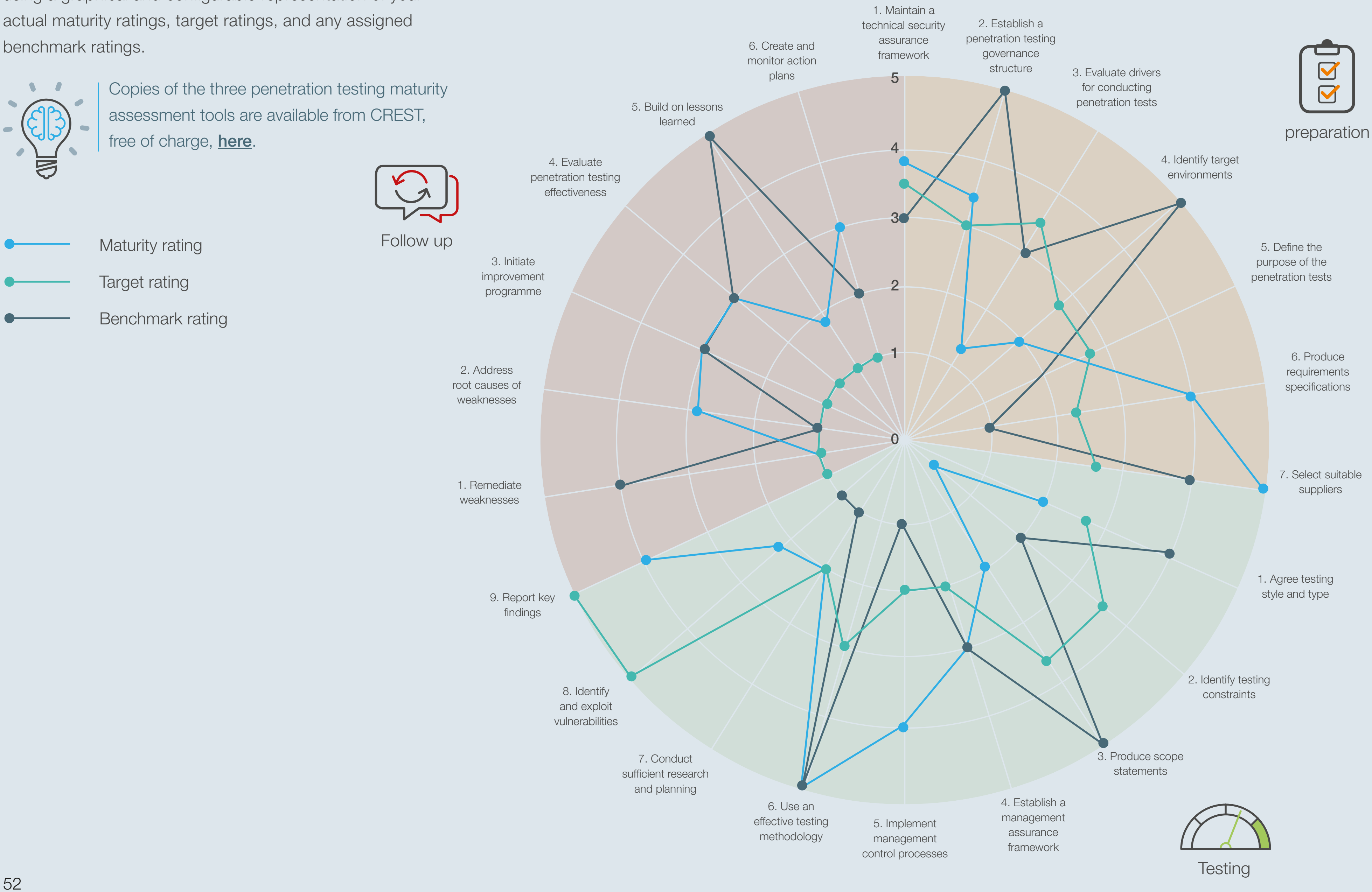
Figure 15: Penetration testing maturity assessment results in bar chart format

	Assessment Level	Maturity level (1 to 5)	Target maturity (1 to 5)	Benchmark rating
Stage A – Preparation		**Maturity level: Level 1**		
Step 1. Maintain a technical security assurance framework	0	🟦🟦🟦 3	🟩🟩🟩 3	4
Step 2. Establish a penetration testing governance structure	0	🟦🟦🟦🟦🟦 5	🟩🟩🟩 3	3
Step 3. Evaluate drivers for conducting penetration tests	0	🟦🟦🟦 3	🟩🟩🟩🟩 4	1
Step 4. Identify target environments	0	🟦🟦🟦🟦🟦 5	🟩🟩🟩 3	2
Step 5. Define the purpose of the penetration tests	0	🟦🟦 2	🟩🟩🟩 3	2
Step 6. Produce requirements specifications	0	🟦 1	🟩🟩 2	4
Step 7. Select suitable suppliers	0	🟦🟦🟦🟦 4	🟩🟩🟩🟩🟩 3	5
Stage B – Testing		**Maturity level: Level 1**		
Step 1. Agree testing style and type	0	🟦🟦🟦🟦 4	🟩🟩🟩 3	2
Step 2. Identify testing constraints	0	🟦🟦 2	🟩🟩🟩🟩 4	1
Step 3. Produce scope statements	0	🟦🟦🟦🟦🟦 5	🟩🟩🟩🟩 4	2
Step 4. Establish a management assurance framework	0	🟦🟦🟦 3	🟩🟩 2	3
Step 5. Implement management control processes	0	🟦 1	🟩🟩 2	4
Step 6. Use an effective testing methodology	0	🟦🟦🟦🟦🟦 5	🟩🟩🟩 3	5
Step 7. Conduct sufficient research and planning	0	🟦🟦 2	🟩🟩 2	2
Step 8. Identify and exploit vulnerabilities	0	🟦 1	🟩🟩🟩🟩🟩 5	2
Step 9. Report key findings	0	🟦 1	🟩🟩🟩🟩🟩 5	4

Results are also shown as a radar diagram, as shown in the example in Figure 16, presenting details to be analysed using a graphical and configurable representation of your actual maturity ratings, target ratings, and any assigned benchmark ratings.

Copies of the three penetration testing maturity assessment tools are available from CREST, free of charge, **here**.

Figure 16: Penetration testing maturity assessment results in radar diagram format



Part 7 – Conclusions

Summary

When activities are planned, performed and reported properly, a penetration test can give you knowledge of nearly all of your technical security weaknesses. It can provide you with the information and support required to fix those vulnerabilities. There are also other significant benefits, which can include:

- A reduction in your long-term ICT costs
- Improvements in the technical environment, reducing support calls
- Greater levels of confidence in the security of your IT environments
- Increased awareness of the need for appropriate technical controls

However, there can be many tricky issues that need to be addressed before conducting a penetration test, to ensure requirements are being properly defined and met. There are also limitations and risks that need to be identified and managed. It is essential to implement an appropriate and effective penetration testing programme.

The way forward

Your organisation can benefit from conducting effective, value-for-money penetration testing. To achieve this, you need to plan for a test, select an appropriate third-party provider, and manage all related activities as part of a penetration testing programme.

Firstly, there are a number of key concepts you need to understand to conduct well-managed penetration tests. These include understanding what a penetration test is (and is not), appreciating its strengths and limitations, and considering why you would want to employ an external penetration testing services provider.

Secondly, to ensure requirements are satisfactorily met, it is advisable to adopt a systematic, structured approach to penetration testing. This involves determining business requirements, agreeing the testing scope and establishing a management framework (including contracts, risk, change and problem management). It should also encompass planning and conducting the test itself and implementing an effective improvement programme.

Finally, if your organisation decides to appoint an external provider of penetration services, it is important that you choose a supplier which most effectively meets your requirements – at the right price. It is often helpful to determine a set of criteria when choosing an appropriate supplier, considering the six key selection criteria outlined in this report.

Further copies of this report are available from CREST, free of charge, **here**.

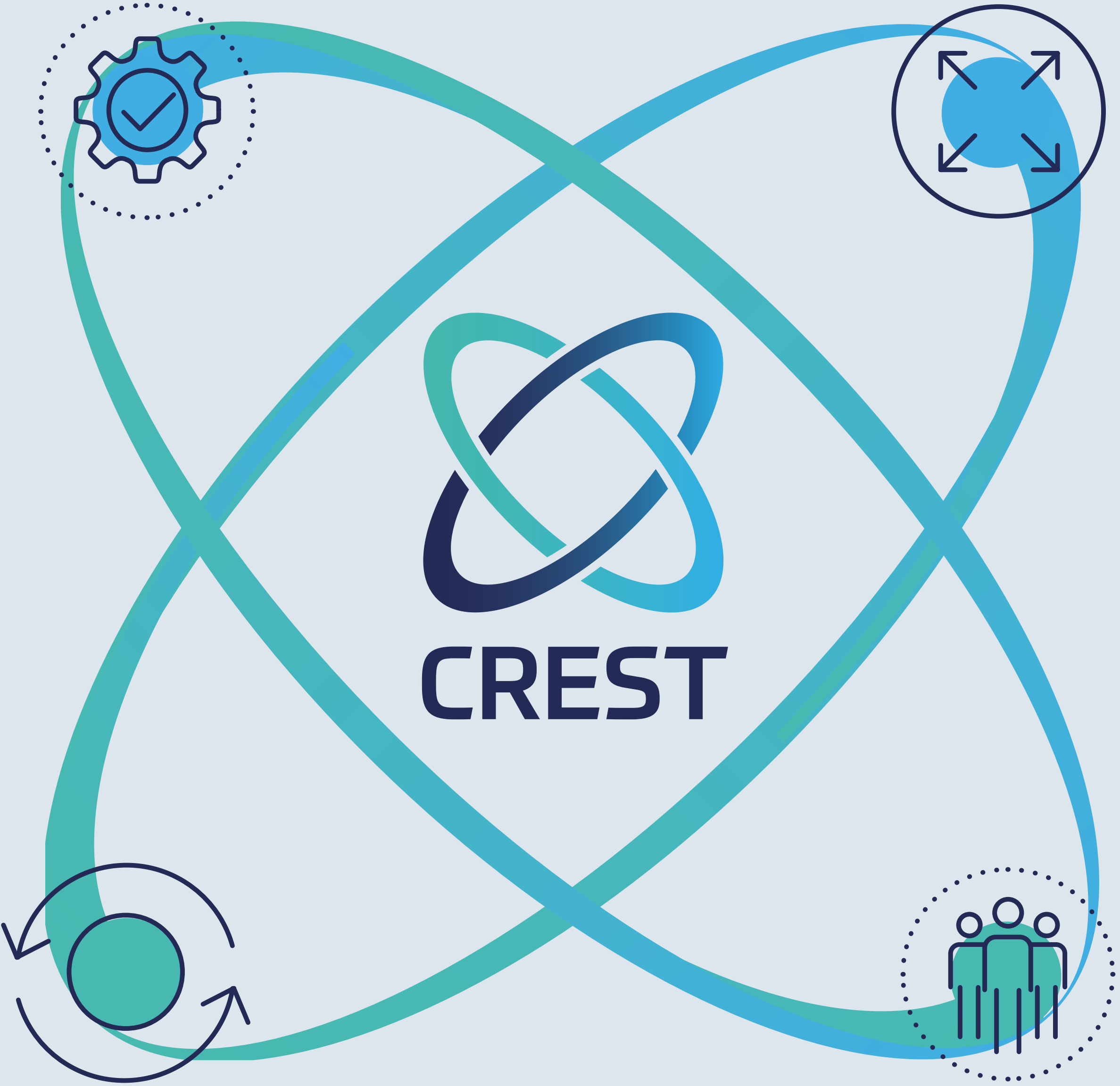
Useful links

CREST penetration testing maturity assessment tools
https://www.crest-approved.org/approved-services/penetration-testing-maturity-assessment-tools/

CREST Defensible Penetration Test
https://www.crest-approved.org/wp-content uploads/2022/12/CREST-Defensible-Penetration-Test-v5-2 pdf

Payment Card Industry Data Standard
https://www.pcisecuritystandards.org/

National Protective Security Authority
https://www.npsa.gov.uk/



Capability

We develop and measure the capability of cyber security organisations and help individuals become increasingly skilled and competent

Capacity

We work across the industry to grow the pipeline of cyber security expertise

Consistency

We set global standards for cyber security organisations to deliver a high quality of service

Collaboration

We develop and engage with the global cyber security community to leverage our shared knowledge and capabilities for the benefit of all

Warning

This Guide has been produced with care and to the best of our ability.
However, CREST accepts no responsibility for any problems or incidents arising from its use.

CREST

For further information contact CREST at:

www.crest-approved.org