



Data Sheet Penetration Testing

Did you know?

The cyber security community and major media largely concur on the prediction that **cyber crime damages will cost the world US\$6 trillion annually by 2021.**

*2016 Cybercrime Report,
Cybersecurity Ventures*

In manual penetration tests, **74% of applications had at least one vulnerability** violating the OWASP Top 10.
2016 NTT Group Global Threat Intelligence Report

Are your critical assets safe from hackers?

Most organisations are the target of random, indiscriminate attacks. Companies typically seek to prevent security breaches with layers of defensive mechanisms, including user controls, cryptography, intrusion/detection systems and firewalls. However, continued adoption of new technologies has made it even harder to discover and remove all of your organisations' vulnerabilities and defend against cyber-attacks.

Without appropriate penetration testing, though, they have no way of ensuring that these defenses provide adequate protection against cyber-attack. A penetration test identifies the vulnerabilities that leave your infrastructure and applications exposed, and gives you the information you need to close any gaps in your security.



Protect • Comply • Thrive

Reduce costs and get accurate results with expert testing

At IT Governance, we offer two levels of penetration test to meet your specific budget and technical requirements:

Level 1

Identifies the vulnerabilities that leave your IT exposed. Combining a series of manual assessments with automated scans, our team will assess the true extent of your system or network's vulnerabilities, allowing you to evaluate your security posture and make more accurate budgetary decisions.

Level 2

Involves **attempting to exploit the identified vulnerabilities** to see whether it is possible to access your assets and resources. This more thorough assessment of your security posture enables you to make more accurate decisions about investing in securing your business-critical systems.

IT Governance uses a tailored approach to ensure the engagement for security testing meets the maturity and expectations of your business. Our fixed-cost packages are ideal for small and medium-sized organisations, or those with no prior experience of security testing. For those with more complex objectives, or that require a more detailed exploration of complex or sensitive environments, our Technical Services team can provide additional expertise through calls or on-site meetings.

Comply with the PCI DSS, ISO 27001, the GDPR and other standards

Conducting regular penetration tests is a component of a number of standards and compliance frameworks, notably the information security standard ISO 27001 and the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS even specifies that scans must include manual testing. Our consultants can produce a structured framework to help you achieve your compliance requirements, and which ensures effective use of your in-house resources and controls expenditure.



What type of penetration test is right for you?

	Level 1	Level 2
Purpose	You need to determine the potential vulnerabilities in target systems	You need to determine whether your business is vulnerable to a hacker and whether you could detect an attack
	You're attempting to identify the solutions required to secure your business in order of priority	
Outcomes	Identify vulnerabilities in your networks, systems, websites, web applications or wireless networks	Tests involve looking at vulnerabilities and trying to gain access to critical resources
	Technical assurance from a CREST accredited information security professional	Technical assurance from a CREST accredited information security professional
Target organisation	You have never undertaken any security testing	You have a mature security programme and want a full test of your network
	You want to go beyond 'light-touch' vulnerability scans or assess your cyber security baseline	You require a real-life threat simulation that establishes your ability to alert and defend
	You are worried that rogue employees or attackers have gained physical access to your internal network	You need to demonstrate high levels of cyber security to your clients
	You need to achieve compliance with a standard, framework or regulation, such as ISO 27001	
Skill level required	High	Advanced
Emulates a real-world attack	No	Yes
Objective	Agreed at outset	Agreed at outset
Fixed-price package	Yes	No
Scoping call with a consultant	Available	Yes
Testing methodology	Threat-driven approach	Threat-driven approach
Vulnerability scanning	Yes	Yes
Can be performed on-site	Yes	Yes
Can be performed remotely	Yes	Yes
Identification of false positives	Yes	Yes
Exploitation of vulnerabilities	No	Yes
Detailed report	Yes	Yes
Manual grading of risk and impact	Yes	Yes
Facilitates compliance with ISO 27001	Yes	Yes
Facilitates compliance with the PCI DSS	Meets the requirements of quarterly internal testing	Meets the requirements of annual internal and external testing

Our methodology

Our team of CREST-accredited consultants will apply robust methodologies to provide you with the technical assurance you need. By adopting a threat-based approach, we can deliver a realistic and targeted appraisal of the current state of your security and the risks attackers pose to your business. We will discuss the results with all relevant audiences and provide recommendations for cost-effective solutions.

1. Initial scoping

Prior to a test, our account management team will discuss your assessment requirements for your systems, networks or applications in order to define the scope of the test.

2. Reconnaissance

During this phase, we will attempt to gather information about your organisation and how it operates. We will use automated scanning to identify potential security holes that could lead to your systems being compromised. *

6. Remediation support

We can provide access to our testers and the raw test data to support and expedite remediation. We can also retest your systems so that you can be sure all the issues have been successfully resolved.

Our methodology

3. Assessment

We will conduct manual tests (e.g. authentication bypass, brute-force attack, public exploits) in an attempt to compromise your system environment and identify attack vectors for your wider network.

5. Presentation







In some instances, we will recommend a separate briefing session with your management team, where we will explain the outcomes of the test and what this means for your security posture, and discuss any further recommendations.

4. Reporting

We will provide a detailed breakdown of all your results in an easily interpreted format based on the damage potential, reproducibility, exploitability, number of affected users, and discoverability of each finding.

* This methodology is fully deployed for a level 2 test, and only partially for a level 1.

Our penetration testing services

Infrastructure		Identifies the resilience of your infrastructure security controls and all the ways an attacker might gain unauthorised access and control	Reports on the security vulnerabilities within your infrastructure that could be exploited in an attack
Applications		Assesses the key components of your web applications and supporting infrastructure, including how these components are deployed and how they communicate with users and server environments	Reports on the security of applications that broker access to critical data
Mobile		Identifies the configuration and deployment flaws associated with integrating mobile solutions into your operating environment and gives detailed remediation advice	Reports on risks from the application on the device, its backend systems, the network it connects to, and the interaction and data flow between them
Wireless		Detects access points and rogue devices, analyses your configurations, and tests for vulnerabilities so that you can implement security controls to prevent an attack	Reports on vulnerabilities, inconsistencies, misconfigurations, and checking for rogue access points
Social		Identifies whether your employees are vulnerable to phishing emails, enabling you to take immediate remedial action to improve your cyber security posture	Reports on the gaps in your internal security awareness and how your organisation reacts to attempts to compromise your staff
IT Healthcheck		Identifies weaknesses in your chosen systems based on widely encountered vulnerabilities and common configuration faults	Reports on the minimum requirements for accreditation in line with HMG Infosec Standard No.2

Our reports

Dealing with the results of a penetration test can be overwhelming; our easy-to-follow reports explain the issues in both plain and technical language.



Executive summary

- Provides a high-level view of risk and business impact
- Can be supplied to end clients as a standalone report



Technical report

- Details the testing methodology
- Delivers a breakdown of the results in an easily interpreted format
- Gives specific remediation advice that will leave you in no doubt about how to fix the identified issues
- Can include raw test data to help with remediation

Why IT Governance?

Our team

Our Technical Services team includes highly-skilled penetration testers who can test your system defenses and websites for vulnerabilities, carry out exploits in a safe manner, and advise on appropriate mitigation measures to ensure that your systems are secure.

We hold a range of accreditations at both a corporate and individual level

Our penetration tests are performed by CREST-accredited security testers, who leverage their diverse knowledge of penetration and vulnerability testing and the associated security challenges to deliver accurate results.

Practical solutions to help you meet your legal, regulatory and contractual requirements

Our expertise in standards such as the PCI DSS, ISO 27001, GDPR and ISO 9001 means we can offer an integrated approach, and can develop suitable solutions that will enable you to reduce your risks and ensure compliance with standards, frameworks, legislation and other business requirements.

Our credentials and corporate certificates:



IT Governance Ltd

Unit 3, Clive Court, Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambs CB7 4EA, United Kingdom

t: + 44 (0) 845 070 1750

e: servicecentre@itgovernance.co.uk

w: www.itgovernance.co.uk

