Risk-X

YOUR DATA. ASSURED.

ASSURANCE – PENETRATION TESTING

Datasheet 1:300

WHAT IS PENETRATION TESTING?

Penetration testing goes beyond that which is covered within a vulnerability assessment. Vulnerability assessment is akin to a burglar "casing the joint" and identifying where the latches on your doors and windows are left open and closed. Whereas, penetration testing will attempt to exploit any discovered weaknesses or, throw a metaphorical brick through the window and bypass any security features altogether. This allows a real-world test of the environment to leverage access to critical system components and sensitive information.

Risk-X base their network layer penetration testing methodology on the NIST Special Publication 800-115 Technical Guide to Information Security Testing and Assessment. For Web application testing the methodology is based on the Open Web Application Security Project (OWASP) Testing Guide v4.

WHAT DO WE OFFER?

INTERNAL - NETWORK

The internal network-layer penetration test is typically conducted on-site, however, depending on the size and scale of the agreed scope, this could be conducted remotely through a device installed on-site. Network layer penetration testing identifies weaknesses with the configuration of hosts, servers and any security flaws due to missing patches or misconfigurations. Vulnerabilities are indexed by version 2 of the Common Vulnerability Scoring System, or are defined as "Information, Low, Medium, High or Critical" by the tester.

Output: Internal penetration test report identifying which IP addresses and host-names are affected, details of the vulnerability, an indication of severity and advice on remediation activities.

PCI Security Standards Council

11.3, 11.3.2, 11.3.3

A.12.6.1, A.13.1.1, A.13.1.2, A.13.1.3, A.14.2.3, A.14.2.8, A.18.2.3

ISO

INTERNAL – NETWORK SEGMENTATION

Network segmentation testing is conducted in order to validate that the network security controls (e.g. VLANs, VRFs, Firewalls) are adequately isolating internal security zones within the network. Ideally, this should be conducted on-site as the tester will require connections to several different network segments; dependent upon the number of security zones being tested. The number of individual tests required is calculated by n*(n–1) where n is the number of network segments.

Output: Internal penetration test report identifying which IP addresses and host-names are affected, details of the vulnerability, an indication of severity and advice on remediation activities.

Option – Contextual awareness

A contextually aware network segmentation review requires the assessed entity to submit documentation such as network diagrams and network port justifications in order to provide some context into the permitted and prohibited traffic between network security zones. The output report will contain additional guidance and recommendations to support the documented network infrastructure.

PCI Security Standards Council

11.3.4, 11.3.4.1

A.13.1.1, A.13.1.2, A.13.1.3, A.14.2.3, A.14.2.8, A.14.2.9, A.18.2.3

ISO

Internal - Wireless

Wireless assessments must be conducted on-site, so that the assessor can get to each of the WLANs. The wireless assessment can cover the following areas:

1. Internal approved wireless network configuration and security;
2. Guest, third party or internet only wireless network configuration and security;
3. Identification of any unauthorised wireless devices at each location being tested;
4. Determining the security status of authorised wireless devices within the defined scope of the test.

Output: A report that details the security practices that are in place, any weaknesses and remediation action items that are required in order to ensure the security of the network and the devices attached.

PCI Security Standards Council: 2.1.1, 4.1.1, 11.1, 11.1.1

ISO: A.12.6.1, A.13.1.1, A.13.1.2, A.13.1.3, A.14.2.3, A.14.2.8, A.18.2.3

Option – Contextual awareness

A contextually aware wireless assessment requires the assessed entity to submit documentation such as network diagrams, details of authorised wireless devices and the CAM tables from the network switches. The tester will use this information to extend the wireless report into the wired environment.

External - Network

The external network-layer penetration test is conducted from the Risk-X secure datacentre against your internet-facing system components. Results will be indexed against version 2 of the Common Vulnerability Scoring System. In addition to this, other aspects of the online presence of the company are tested to verify that public documents are stripped of any potentially useful metadata or sensitive information, DNS records and public information gained through search engines cannot be used to bypass any security functionality on employee portals such as webmail, VPNs or collaborative software. These other areas will be defined as "Information, Low, Medium, High or Critical" by the tester, using their judgement and experience based on the risk posed to your business.

Output: External penetration test report identifying which IP addresses and host-names are affected, details of the vulnerability, an indication of severity and advice on remediation activities.

PCI Security Standards Council: 11.3, 11.3.1, 11.3.3

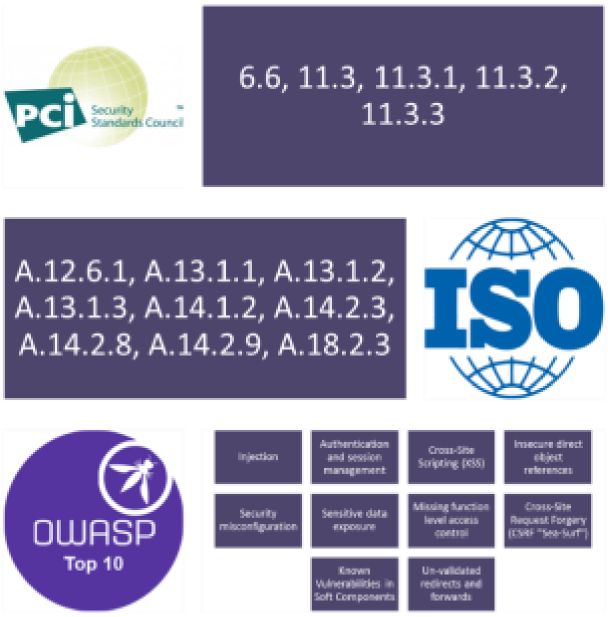
ISO: A.12.6.1, A.13.1.1, A.13.1.2, A.13.1.3, A.14.1.2, A.14.2.3, A.14.2.8, A.14.2.9, A.18.2.3

Web Application

External Web application testing is conducted from the Risk-X secure datacentre and aims to identify application layer vulnerabilities. Throughout the testing process the application will be subject to both automated and manual tests, and the tester will determine if the application is susceptible to the Open Web Application Security Project (OWASP) top-10 list of application vulnerabilities, often referred to as the OWASP top 10. Further testing is available for specialist areas including the OWASP mobile top 10, SANS, NIST or compliance framework based testing.

This test can also be completed for internal web applications through a device installed on-site. Our testers can then evaluate the web application from an insider's perspective.

Output: The Risk-X web application vulnerability assessment report will provide you with an in-depth view of the application and how the tester managed to compromise the application, as well as providing remediation advice on how to correct any issues found.



6.6, 11.3, 11.3.1, 11.3.2, 11.3.3

A.12.6.1, A.13.1.1, A.13.1.2, A.13.1.3, A.14.1.2, A.14.2.3, A.14.2.8, A.14.2.9, A.18.2.3

Injection
Authentication and session management
Cross-Site Scripting (XSS)
Insecure direct object references
Security misconfiguration
Sensitive data exposure
Missing function level access control
Cross-Site Request Forgery (CSRF "Sea-Surf")
Known Vulnerabilities in Soft Components
Un-validated redirects and forwards

Each of the tests that we offer in this area can be customised around your requirements and as required in line with CREST methodologies as well as those of NIST and OWASP. Each of these penetration tests can be conducted in blind, unauthenticated and authenticated modes, as follows:

Blind Testing (i.e. Black Box)	Blind testing is conducted where the assessed entity shares no information with the tester. There is no specific defined scope, however there is a time restriction based upon the number of testing days purchased by the assessed entity. Blind testing is only conducted as an internal test, unless we are doing reconnaissance only. This is due to the inevitability of a blind external penetration test resulting in a violation of the Computer Misuse Act.
Unauthenticated Testing (i.e. Grey Box)	Unauthenticated testing is conducted where the assessed entity does not share any credentials with the tester. The scope of the test is defined by the IP addresses and URLs agreed before the test commences. The penetration test covers the ports, protocols and services which can be enumerated and leveraged by the tester. They then try to break in without being authenticated just as an attacker would.
Authenticated Testing (i.e. White Box)	Authenticated testing is conducted where the assessed entity provides authentication credentials to the tester. The penetration tester can then login to system components which provides a more detailed report on the patching and configuration of the system components within the scope of the assessment. This is usually done with "user" level access permissions with the intent that the tester will attempt to leverage vulnerabilities in order to gain privileged access to system components and sensitive data.

There is one other option that is available, and one that is quite popular amongst our clients as it provides the best of all worlds, and this is the hybrid test. A hybrid test allows for the following:

HYBRID	One of the areas that our testers have the most success is with the hybrid test. This allows us to work through the all of the methodologies above. We start with blind testing, and when we find information we assess how long it would take to crack. You then provide us with that information, and the tester moves on. This provides significant efficacy and efficiency of testing as it reduces the testers time on the mundane tasks that are time consuming and inefficient. It also provides you with significant information on how much data is available, what it can be used for, how long each penetration would take and how/if you could respond to each of the areas found.

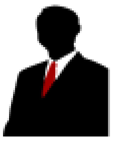
Penetration testing can be a complex process, but our testers are real people as well as consultants, so they can explain to you the exact nature of the issues found, and how you can fix them. This won't just be parrot fashion of what the manufacture says either. During the process of the test you can also work with our testers to see what they do and how they do it, and anything critical we will discuss with you during testing. Once you have the report we will do a debrief call or meeting with you to cover any issues or questions that you may have. You can also contact the team after your test to discuss any issues or clarifications about the remediation actions provided.

WHY RISK-X?

Risk-X provides this service to commercial customers as well as those in high risk areas of gambling and insurance. You have never heard of these companies or seen them in the news, as they use our services to stay secure! It is no longer a case of if but when and how badly. Our consultants are real people and the team has skills across testing, forensics, ISO27001 implementation and PCI DSS so we can provide real world testing and pragmatic remediation. If the team spots a breach or potential breach, we are best placed to use our forensic services to confirm if this has occurred, and can help you throughout the criminal and legal processes. Talk to us today about how we can help you….

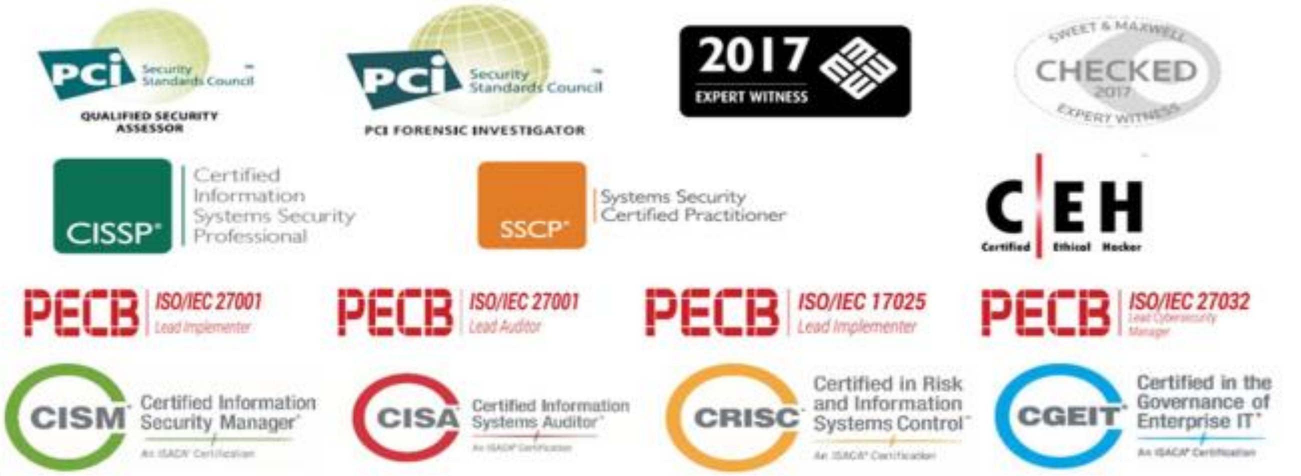
Key contacts

Andrew Gilhooley
Managing Director Assurance
Andrew.gilhooley@risk-x.co.uk
+44 7580 834586



John Martin
Principal Tester
john.martin@risk-x.co.uk
+44 7736 636050

Qualifications - Company


PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR
PCI Security Standards Council
PCI FORENSIC INVESTIGATOR
2017 EXPERT WITNESS
SWEET & MAXWELL CHECKED 2017 EXPERT WITNESS
CISSP Certified Information Systems Security Professional
SSCP Systems Security Certified Practitioner
C|EH Certified Ethical Hacker
PECB ISO/IEC 27001 Lead Implementer
PECB ISO/IEC 27001 Lead Auditor
PECB ISO/IEC 17025 Lead Implementer
PECB ISO/IEC 27032 Lead Cybersecurity Manager
CISM Certified Information Security Manager An ISACA Certification
CISA Certified Information Systems Auditor An ISACA Certification
CRISC Certified in Risk and Information Systems Control An ISACA Certification
CGEIT Certified in the Governance of Enterprise IT An ISACA Certification

Risk-X is a trading name of Risk-X LLP, Registered in England at Chandos House, School Lane, Buckinghamshire, MK18 1HD. Partnership Number OC366692