



# We are <sup>PCI</sup> Penetration Testers • Full Stop •

Many organisations do not realise that PCI DSS Requirements 6.6 and 11.3 call for penetration testing over and above the external and internal vulnerability assessments required by PCI DSS Requirement 11.2.



- Ethical
- 
- Pragmatic
- 
- Professional

## The PCI SSC's document "Information Supplement: Penetration Testing" says:

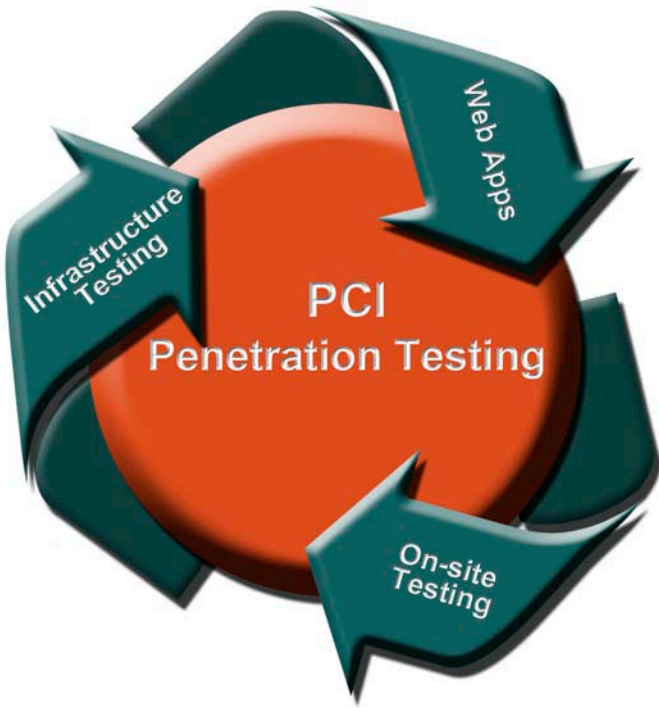
*"A vulnerability assessment simply identifies and reports noted vulnerabilities, whereas a penetration test attempts to exploit the vulnerabilities to determine whether unauthorised access or other malicious activity is possible. Penetration testing should include network and application layer testing as well as controls and processes around the networks and applications, and should occur from both outside the network trying to come in (external testing) and from inside the network."*

What Tests are required?	Frequency	ASV/QSA Required?	Location
Web Application Test	Annual	No	Remote
External Penetration Test	Annual	No	Remote
Internal Penetration Test	Annual	No	On Site

### ...in addition:

*"Penetration testing must be carried out at least annually and anytime there is a significant infrastructure or application upgrade or modification (for example, new system component installations, addition of a sub-network, or addition of a web server). What is deemed "significant" is highly dependent on the configuration of a given environment, and as such cannot be defined by PCI SSC. If the upgrade or modification could impact or allow access to cardholder data, then it should be considered significant. Significance within a highly segmented network where cardholder data is clearly isolated from other data and functions is very different than significance in a flat network where every person and device can potentially access cardholder data. As a security best practice, all upgrades and modifications should be penetration-tested to ensure that controls assumed to be in place are still working effectively after the upgrade or modification."*

PCI DSS Testing Services



This is where we come in - because we are <sup>PCI</sup> penetration testers • Full Stop •



# We are <sup>PCI</sup> Penetration Testers • Full Stop •



Ethical

Pragmatic

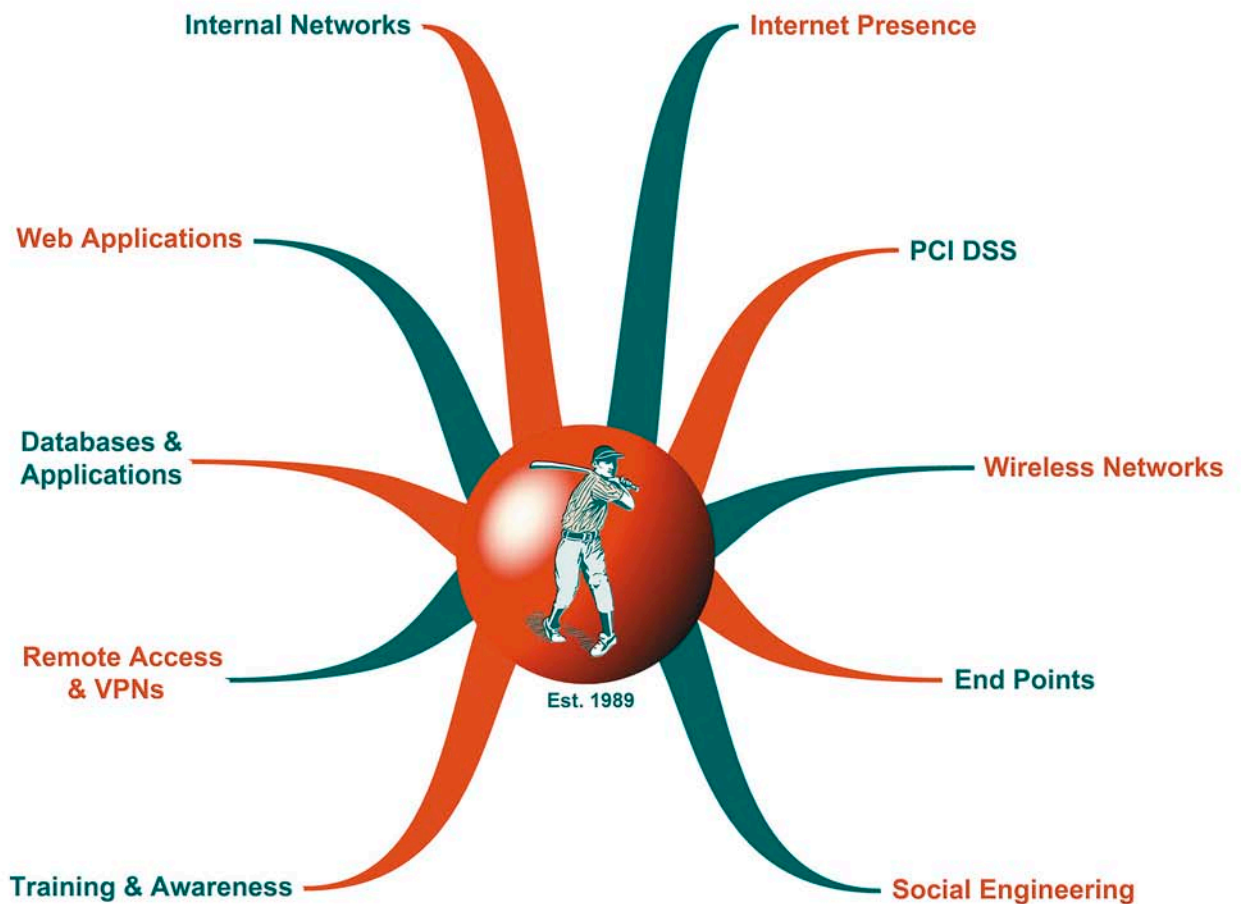
Professional

<sup>PCI</sup>  
**First Base Technologies** penetration testing solution:

- 1 Our web application tests comply with PCI DSS requirement 6.6 "Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes."
- 2 Our external and internal penetration tests comply with PCI DSS requirement 11.3 "Penetration testing should include network and application layer testing as well as controls and processes around the networks and applications, and should occur from both outside the network trying to come in (external testing) and from inside the network."

**Here's what we can test to help you meet your PCI DSS requirements:**

PCI DSS Testing Services



Get your quote now

Call Andy on +44 1273 45 45 25 or e-mail [info@firstbase.co.uk](mailto:info@firstbase.co.uk)