PENETRATION TESTING

Perspective Risk

Buyer’s Guide
WHAT SHOULD I LOOK FOR IN A PROVIDER OF PENETRATION TESTING SERVICES?

Does the provider have the capability and is this capability independently verified to any standard?

Providers that are serious about the quality of their penetration testing demonstrate this by undergoing independent verification.

In the UK, this means allowing CREST, a not-for-profit information security standards authority, to scrutinise a company’s penetration testing and supporting processes. To maintain standards, CREST carry out annual assessments.

If you are in the public sector or if you supply to government, look for a company that has been accredited by the National Cyber Security Centre (NCSC) as a CHECK Green Light service provider.

Similar to CREST, the NCSC CHECK scheme gives buyers confidence that a provider’s penetration testing services have been measured against rigorous government standards.

Does the company practice what it preaches?

Invariably, penetration testing means that the penetration testers will come into contact with your sensitive data. How can you be confident they will look after it? Without auditing the provider yourself, which can be time consuming, how can you trust their capabilities?

A provider that has been independently certified to well-known standards should provide the necessary assurance. ISO 27001 certification, and where penetration testing services are referenced expressly, is one such standard to look out for.

Have other buyers bought and have they been happy with the service?

Ask for references and look for testimonials and case studies. Confident providers will seek and share feedback because they are committed to delivering a quality service.

They are not afraid of losing clients, because why would they want to go elsewhere? Regular customer satisfaction feedback is also a great way of keeping penetration testers on their toes.

HAPPY WITH THE COMPANY? TAKE A LOOK AT ITS PEOPLE

What should you look for in a Penetration Tester?

As with quality providers, reputable penetration testers will themselves undergo periodic checks of their status and qualifications.

The CREST and NCSC CHECK schemes afford the means to validate a pen tester’s skill set.

Look for these qualifications, check out CREST’s website to see which level is best suited to your needs: UK CREST Member Companies Supplying Penetration Testing Services

Or, for the CHECK Scheme: National Cyber Security Centre Professional services

Verify their CREST certification claims: How to verify a CREST Qualification

Verify their CHECK certification claims: National Cyber Security Centre - Using a CHECK provider
So, they can carry out a professional penetration test, what about their ethics?
Do the testers have criminal records? Might they be tempted to steal or cause harm? You should gain assurances that the provider has made every effort to verify and vet its employees.

Ask about the provider’s vetting processes. Are they done by independent screening companies or in-house? Third party screening avoids bias. It would be prudent to include all personnel involved in the delivery of services and not solely the penetration testers.

This should include background checks of employment, professional and school qualifications, and most importantly a criminal record check.

If you are a supplier to government, this should include verifying the government Security Clearance of individuals. As a minimum, look for SC or DV (Developed Vetting) clearance.

Does the provider employ full time testers or is the work contracted out?
Some providers are mere sales fronts, reliant on contractors to deliver penetration testing. How can they mandate the quality, ethos and ethics of their hired hands?

Compared to staff, contractors have less to lose as they can walk away to another contract. Employees are more accountable for the service they give, having committed themselves to the business, its cause and its standards. Greater care and attention to detail can normally be expected from employees.

What are the costs?
Expect them to be variable. Penetration Testing is usually sold by the day. Essentially, you are purchasing the time and skills of a penetration tester to provide the information you need.

A penetration tester’s man day typically costs anywhere between £600 and £2,000, exclusive of VAT and travel expenses.

Anything above £1,000 per day and you will be paying a premium for the brand. Nothing wrong with that if you have sensitive stakeholders and want to highlight that you have not skimped by going for a well-known name.

If it is a premium service you are after rather than a premium brand, use the above figures to help you make your decision.

Need to verify the quotes you have received? Obtain prices from three reputable providers. The content of their quotes or proposals will give you an idea of how much care they have taken to listen to you and understand your requirements.

Use our buyer’s checklist templates at the end of this guide to record your notes and price comparisons.

If you merely receive a pricing table, you may well get you pay for!

COMPANY AND PEOPLE ALL GOOD? TAKE A LOOK AT WHAT THEY DELIVER

What are you actually buying? A Pen Test or a Vulnerability Scan?
A vulnerability scan is largely an automated process for assessing computers, networks and applications etc. for security weaknesses.

Ask your potential provider for their penetration testing methodology or a summary of their process. This will ensure you are signing up for a comprehensive threat-based penetration test and not a vulnerability scan dressed up as one.

Be wary of 'appliances' promising efficiencies and savings as you may well receive a vulnerability scan in a prettified report.

Have they listened and have they understood?
To ensure your security objectives are met, your provider should furnish you with a scoping document; the blueprint for the penetration test.

A fluffy scope could end up being a costly mistake. The provider should detail your expectations and requirements and capture relevant impacts and potential threats. Without knowing these values, risk cannot be accurately calculated.

There should be no shadow of doubt as to:

- What is being tested
- How it is being tested
- Why it is being tested
- Who is doing the testing
- Where the testing is taking place

Sound penetration testing is a collaborative exercise. If it’s delivered in an uncontrolled or unprofessional fashion it could leave you with a lot of cleaning up to do afterwards.

Your provider will require assistance to set up your system or network in readiness for the penetration test and making the relevant personnel aware of it.

All these requirements and prerequisites should be formally captured and communicated in the scope document.
Can you understand the results?

There are many talented penetration testers who can hack into most systems, but can they communicate their findings in a way you and your colleagues will understand?

The Pen Test Report is the tangible deliverable you will receive after a penetration test.

**Key things to look out for:**

- Is there a management summary directed at non-technical people? The findings should promote wider discussions about business risk and impacts, and not be limited to threats and vulnerabilities.

  Equally, some reports merely describe vulnerabilities without any technical terminology. Consequently, the value of the penetration test is lost at key decision maker level, together with the messages that need to be conveyed and understood by executives.

- Is there a technical summary giving an aerial view of the overall threat and vulnerability landscape for the target systems? Is it meaningfully set out?

  The threats your organisation is vulnerable to should be prioritised. This is sometimes done in tabulated form with a RAG (Red, Amber, Green) system.

- Are the vulnerabilities reported in sufficient detail? Is there enough information for you to understand their impact and risk? Are steps included to allow you to recreate them or is the provider hiding behind a ‘black art’?

  Is there detailed remediation information? Is it customised to your systems, or is it a generic one line statement along the lines of “provider recommends you fix it”?

A quality provider of penetration testing services should happily and quickly provide you with sample reports. They are necessary for the independent annual accreditation process for penetration testing, so will be on hand.

To protect their intellectual property and the information you exchange with them, good providers will request a mutual non-disclosure agreement.

Ask for sample documentation to see if, as a minimum, it addresses all the above points.
WHO IS PERSPECTIVE RISK?

Perspective Risk is a specialist, vendor agnostic, provider of information security services. Our penetration testing services and our testers are accredited annually by CREST and CHECK.

You can read about our directors here.

Accreditations

You can check our accreditations here:
CREST Perspective Risk
And here:
National Cyber Security Centre Perspective Risk
CHECK service

Certifications

We distinguish ourselves in the industry by working with our clients as an extension of their team. Our approach is collaborative; we like to guide and upskill at the same time.

Quality and our customers lie at the heart of everything we do; we aim to exceed expectations and delight.

Perspective Risk maintains certifications to international standards including ISO 9001 (quality) and ISO 27001 (security). Our certifying body is QMS International plc.

Testimonials

“We’d recommend Perspective Risk in a heartbeat. The responsiveness of PR was great. They responded well to our needs, regularly made contact and provided helpful assistance.”

Mark Devis, Head of Technology, Christians Against Poverty

“Perspective Risk stand out in the field of penetration testing because they understand the importance of security risks and are able to map it to the domain in which their client is operating.

“Their service is very much tailored to the particular application being examined. Simply using automated scanning tools is not a replacement for smart, intelligent people with a deep understanding of security related issues.

“Perspective Risk take penetration testing to the next level, using real people to test systems and interpret the results.”

Pete Hanlon CTO, MoneySupermarket.com Group Plc

“A pleasure to work with and not only delivered more than I expected but are continuing to assist with our security plan.”

Tony McGivern, IT Security Specialist, County Durham & Darlington NHS Foundation Trust

“I would like to commend the work of Zia, who was an excellent and diligent point of contact before, during and after the test. His good work is the reason behind the 5/5 scores.”

Olivier Thereaux, Senior Technologist, BBC

To read more about what our customers are saying about us, please click: Perspective Risk Client Testimonials.
Some examples of the reports you can expect from Perspective Risk

Our reports are wrapped around your needs and customised to suit. For example, you may have explicit security concerns and require us to test specific systems. Deficiencies against particular standards can be highlighted, together with remediation advice.

Alternatively, your scope is broad and you want our team to identify and prioritise the vulnerabilities across your infrastructure and what the key threats are.

See below for a highlight of what our reports include:
Detailed Risk Description

4.2 Session Information Transmitted without Encryption

Control: Session Management  
Targets: Supporting Web Services  
High

4.2.1 Impact

The supporting Acme web services offer functionality over both HTTP (unencrypted) and HTTPS (encrypted) connections. As the same cookie is used for both these connection types it would be possible for an attacker in a position to observe network traffic to intercept the unencrypted HTTP cookie transmissions and use the cookie to gain access to authenticated sections of the application, whereby personal and financial data can be viewed.

4.2.2 Probability

As mobile devices are commonly used over shared Wi-Fi connections such as hotels, airports etc., intercepting data becomes trivial and thus the probability of this attack being realised is high. Tools are freely available for the interception of data over Wi-Fi and little or no skill is required for their use. Once session tokens are obtained by these means an attacker must have a degree of knowledge to use them to steal a user session however attacks of this nature are well publicised on the Internet.

4.2.3 Remediation

If feasible it is recommended that the entire application including unauthenticated pages, such as news, events and help pages be transmitted over HTTPS and the HTTP service be disabled. If this is not possible and a HTTP service is functionally required the application should redirect any requests for sensitive content back to the HTTPS service.

Furthermore, the Secure cookie attribute should be implemented on all authenticated cookies to prevent them being sent to HTTP pages, such as the news, event and help pages. This should be reinforced using cookie scope instructions to prevent tokens being submitted for these resources.

The following instructions relate to configuring the Secure cookie flag in the PHP technology in use on the application:

Cookie parameters can be configured framework wide within the php.ini file or they can be configured on a per script basis.

Setting the Secure flag in the php.ini file is as simple as inserting the following directive:

```
session.cookie_secure = True
```

To set the Secure flag on a per script basis, i.e. before each session_start() call:

```
void session_set_cookie_params ( int $lifetime [, string $path [, string $domain [, bool $secure= true [, bool $HttpOnly= true ]]]]])
```

4.2.4 Technical Details

Initial access to the application does not require authentication allowing for a user to browse the latest news, events and product offerings and view help files. This communication takes place over HTTP:

URL being accessed: http://www.example.com/Events
Cookie set: _acme_session=76gjtcft8p9oe2rm8w76gflps9

Get in Touch

Would you like a complete example report? Drop us a line.

If you would like a penetration test, some friendly advice, or even just to sanity check another provider’s claims, we will be glad to assist. You will not be obligated or pressured in the least; that is not how we do business!

Coverage throughout the UK.

London: 020 0200 8142
Northampton: 01604 882 882
Leeds: 0113 880 0722
Email: info@perspectiverisk.com

Or enter your details directly onto our contact form
# Buyer's Checklist

Feel free to use these templates to note your findings:

**PROVIDER:**

**CONTACT NAME:**

<table>
<thead>
<tr>
<th>Question</th>
<th>Hints</th>
<th>Your Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do they have the capability to perform a penetration test?</td>
<td>Look for membership of CREST and CHECK</td>
<td></td>
</tr>
<tr>
<td>Practice what they preach?</td>
<td>Look for ISO certifications (ISO 27001 and ISO 9001)</td>
<td></td>
</tr>
<tr>
<td>What do other buyers say?</td>
<td>Look for testimonials and references</td>
<td></td>
</tr>
<tr>
<td>Consultants qualified?</td>
<td>Look for CREST and CHECK qualifications</td>
<td></td>
</tr>
<tr>
<td>Consultants thoroughly vetted?</td>
<td>Look for independent vetting certificates and security clearances</td>
<td></td>
</tr>
<tr>
<td>Are the consultants full time employees?</td>
<td>Make sure they don't use contractors, who are much harder to control</td>
<td></td>
</tr>
<tr>
<td>Pen Test or Vulnerability Scan?</td>
<td>Ask whether their approach is manual or automated</td>
<td></td>
</tr>
<tr>
<td>Fully understood your requirements?</td>
<td>Ask how they document your requirements. See if they take into account more than just “target” information. They need to understand your concerns and risk profile</td>
<td></td>
</tr>
<tr>
<td>Sample reports available?</td>
<td>Have a look at their samples. Can you understand them?</td>
<td></td>
</tr>
</tbody>
</table>

## NEED HELP?

Coverage throughout the UK.

**London:** 020 0200 8142  
**Northampton:** 01604 882 882  
**Leeds:** 0113 880 0722  
**Email:** info@perspectiverisk.com  
Or enter your details directly onto our contact form
# Buyer’s Checklist

Feel free to use these templates to note your findings:

**PROVIDER:**

**CONTACT NAME:**

<table>
<thead>
<tr>
<th>Question</th>
<th>Hints</th>
<th>Your Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do they have the capability to perform a penetration test?</td>
<td>Look for membership of CREST and CHECK</td>
<td></td>
</tr>
<tr>
<td>Practice what they preach?</td>
<td>Look for ISO certifications (ISO 27001 and ISO 9001)</td>
<td></td>
</tr>
<tr>
<td>What do other buyers say?</td>
<td>Look for testimonials and references</td>
<td></td>
</tr>
<tr>
<td>Consultants qualified?</td>
<td>Look for CREST and CHECK qualifications</td>
<td></td>
</tr>
<tr>
<td>Consultants thoroughly vetted?</td>
<td>Look for independent vetting certificates and security clearances</td>
<td></td>
</tr>
<tr>
<td>Are the consultants full time employees?</td>
<td>Make sure they don’t use contractors, who are much harder to control</td>
<td></td>
</tr>
<tr>
<td>Pen Test or Vulnerability Scan?</td>
<td>Ask whether their approach is manual or automated</td>
<td></td>
</tr>
<tr>
<td>Fully understood your requirements?</td>
<td>Ask how they document your requirements. See if they take in to account more than just “target” information. They need to understand your concerns and risk profile</td>
<td></td>
</tr>
<tr>
<td>Sample reports available?</td>
<td>Have a look at their samples. Can you understand them?</td>
<td></td>
</tr>
</tbody>
</table>

**NEED HELP?**

Coverage throughout the UK.

**London:** 020 0200 8142  
Northampton: 01604 882 882  
Leeds: 0113 880 0722  
Email: info@perspectiverisk.com

Or enter your details directly onto our contact form.
# Buyer’s Checklist

Feel free to use these templates to note your findings:

**PROVIDER:**

**CONTACT NAME:**

<table>
<thead>
<tr>
<th>Question</th>
<th>Hints</th>
<th>Your Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do they have the capability to perform a penetration test?</td>
<td>Look for membership of CREST and CHECK</td>
<td></td>
</tr>
<tr>
<td>Practice what they preach?</td>
<td>Look for ISO certifications (ISO 27001 and ISO 9001)</td>
<td></td>
</tr>
<tr>
<td>What do other buyers say?</td>
<td>Look for testimonials and references</td>
<td></td>
</tr>
<tr>
<td>Consultants qualified?</td>
<td>Look for CREST and CHECK qualifications</td>
<td></td>
</tr>
<tr>
<td>Consultants thoroughly vetted?</td>
<td>Look for independent vetting certificates and security clearances</td>
<td></td>
</tr>
<tr>
<td>Are the consultants full time employees?</td>
<td>Make sure they don’t use contractors, who are much harder to control</td>
<td></td>
</tr>
<tr>
<td>Pen Test or Vulnerability Scan?</td>
<td>Ask whether their approach is manual or automated</td>
<td></td>
</tr>
<tr>
<td>Fully understood your requirements?</td>
<td>Ask how they document your requirements. See if they take in to account more than just “target” information. They need to understand your concerns and risk profile</td>
<td></td>
</tr>
<tr>
<td>Sample reports available?</td>
<td>Have a look at their samples. Can you understand them?</td>
<td></td>
</tr>
</tbody>
</table>

---

**NEED HELP?**

Coverage throughout the UK.

**London:** 020 0200 8142  
**Northampton:** 01604 882 882  
**Leeds:** 0113 880 0722  
**Email:** info@perspectiverisk.com  
Or enter your details directly onto our contact form