Penetration Testing

Essential guide

Uncover hidden vulnerabilities and build resilience with **penetration testing**

LRQA

LRQA

SECURITY TESTING

Contents

Introduction

In 2025, cyber risk sits squarely on business agendas – a single breach can erase customer trust, trigger regulatory fines and knock millions off market value. Automated scanners alone no longer keep pace with cloud-native, AI-enabled and supply-chain attack paths. Focused penetration testing remains the most effective way to prove which controls really withstand a motivated adversary – and which merely look good on paper.

An average penetration testing engagement costs around £7,500. Compare this with USD 4.9 million[1] – the average cost of a data-breach – and it's clear that proactive testing is still an exceptionally cost-effective control.

As the only provider in the world holding the full suite of CREST accreditations – and winner of TEISS Best Pen Test Service 2024 – LRQA couples manual exploitation skill with threat-intel-driven scoping to surface material risks in days, not months.

The pages that follow explore today's threat landscape, clarify what the regulators expect and map out LRQA's step-by-step approach to planning, conducting and measuring truly effective penetration testing.

1 | *IBM – Cost of a Data Breach Report 2024. www.ibm.com/reports/data-breach*

The 2025 threat landscape

Global cyber-crime is now valued at about USD 10.5 trillion a year, effectively making it the world's third-largest economy[2]. Four developments explain the surge.

Ransomware remains the blunt weapon of choice

UK incidents climbed 70% in 2024 and ransom demands averaged USD 2.73 million[3,4]. Because modern ransomware gangs both encrypt and steal data, an effective penetration test must simulate exfiltration as well as lock-out.

AI-enabled deception scales fast

87% of organisations have already faced AI-powered attacks. 95% of security leaders report multichannel campaigns that hop from email to chat to voice within minutes[7]. Penetration tests now need to include deepfake voice and cross-platform social-engineering scenarios.

Software-supply-chain compromise amplifies impact

Attacks on upstream vendors rose a third last year, affecting 183,000 customers in a single 12-month span. Gartner expects almost half of all organisations to experience such a breach by 2025[5,6]. Red and Purple Team exercises that probe CI/CD pipelines are becoming mandatory for mature programmes.

Cloud misconfiguration remains the Achilles heel

Misconfigured services account for 68% of cloud security issues. Analysts still expect 99% of cloud failures to be customer-driven by 2025[8,9]. Cloud-specific penetration tests expose IAM privilege creep, serverless exposure and container breakouts that scanners routinely miss.

Underpinning every vector is the human element

Studies show people contribute to the majority of breaches and skills gaps continue to widen[10,11]

2 | *Cobalt – Top Cybersecurity Statistics for 2025. www.cobalt.io/blog/top-cybersecurity-statistics-2025*

3 | *AnSecurity – UK Cybersecurity Statistics 2025 – Navigating the Evolving Threat Landscape. www.ansecurity.com/uk-cybersecurity-statistics-2025-navigating-the-evolving-threat-landscape*

4 | *Fortinet – Cybersecurity Statistics 2025: Rising Threats and Industry Impact (ransomware & AI figures). www.fortinet.com/uk/resources/cyberglossary/cybersecurity-statistics*

5 | *SentinelOne – Cyber Security Statistics 2025 (supply-chain attack growth). www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics*

6 | *Gartner – Innovation Insight for Secure Software Supply Chain 2025 (forecast quoted via Fortinet). www.fortinet.com/uk/resources/cyberglossary/cybersecurity-statistics#supply-chain*

7 | *Verizon – 2025 Data Breach Investigations Report (cloud-misconfiguration share). www.verizon.com/business/resources/reports/dbir*

8 | *Palo Alto Networks – Cloud Security Report 2025 (54 percent exposed workloads). www.paloaltonetworks.com/resources/research/cloud-security-report*

9 | *Gartner – Forecast: Public Cloud Services, Worldwide, 2023-2029 (99 percent customer-driven failures). www.gartner.com/en/documents/3985733*

10 | *(ISC)² – Cybersecurity Workforce Study 2024/25 (skills-gap statistic). www.isc2.org/Research/Workforce-Study*

11 | *UK Government – Cyber Security Breaches Survey 2025 (human-element share of breaches). www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025*

Why penetration testing remains essential

Automated scanners and routine compliance checks form an important baseline, but they only tell part of the story. Real attackers blend cloud misconfigurations, bespoke code flaws and social-engineering tactics that evade generic tools. Penetration testing emulates those adversaries to expose the vulnerabilities that matter most.

Recent LRQA engagements have consistently uncovered exploitable gaps that automated tools miss – giving organisations the deep, actionable insight they need to shore-up defences.

Laws, regulations and standards keep raising the bar

Many laws, regulations and standards now mandate or recommend vulnerability assessment (VA) and/or penetration testing (PT). The table highlights key regimes and their requirements.

It is important to understand that these types of assurance are not interchangeable. Regulators now judge, not only whether testing has occurred, but also whether its scope, methodology and remediation cycle are proportionate to business risk.

Standard	Vulnerability assessment	Penetration testing
PCI DSS	Required	Required
ISO/IEC 27001	Recommended	Recommended
SOC 2	Recommended	Recommended
DORA (EU)	Required	Required
GDPR (EU, UK)	Recommended	Recommended
CHECK Scheme (UK)	Required as part of penetration testing	Required
SSAT (Singapore)	Required	Required
MAS TRM (Singapore)	Required	Required
I-CRT (Canada)	Required	Required
NIST SP 800-115 (USA)	Required	Required
HIPAA (USA)	Recommended	Recommended
NIST SP 800-115 (USA)	Recommended	Recommended

Why penetration testing remains essential

Interpretation and scope rationale

Under the NCSC's CHECK scheme, automated tools may be used to improve coverage, but heavy reliance on those tools without sufficient manual interpretation will not meet standards. CREST also requires accredited testing providers like LRQA to document the rationale for their chosen scope and approach, aligned to the client's specific requirements.

Reputation, customer trust and ESG reporting

Market research shows that publicised breaches erode customer confidence and invite intense scrutiny from investors and the media. ESG disclosure frameworks increasingly expect boards to demonstrate how they protect personal data. A structured penetration testing programme provides objective, third-party evidence that security controls genuinely stand up to real-world attack techniques.

What a penetration test *is* and what it *isn't*

A penetration test is a deliberate, legally sanctioned attempt to breach agreed systems so genuine weaknesses can be fixed before real attackers exploit them. It goes well beyond an automated vulnerability scan by combining manual, context-driven techniques under a predefined scope, objectives, data-handling rules, reporting, retesting and lessons-learned activities. Omitting any of these elements risks blind spots and a false sense of security."

– ***Tom Wedgbury,*** *Managing Principal Security Consultant, LRQA*

Beyond scan-and-report:
Why ‘just running a test’ falls short

The illusion of coverage

Many organisations treat a penetration test as a one-off compliance chore: launch an automated scanner, generate the PDF, then file it away. The document often lists dozens of surface-level weaknesses yet offers no insight into which ones matter. Boards assume the estate is covered, but the same issues resurface a year later because nothing meaningful was fixed.

No feedback loop

When a report ends at vulnerability description, security teams are left guessing which fixes should come first.

Effective programmes include a live debrief, a remediation workshop and a retest window that proves the fixes work. Without that cycle, even the best recommendations gather dust and the organisation slips back into reactive patching.

Missed business context

A checklist engagement rarely shows how an attacker could chain seemingly minor misconfigurations – an overlooked storage bucket here, a stale user account there – to reach business critical data. Only a focused test, steered by skilled operators, traces those paths end-to-end and translates findings into real business impact.

Risk-led scope versus blanket scope

A blanket ‘test everything’ brief spreads effort too thin, while a narrow focus on public IP ranges can miss critical paths such as authentication providers or lateral movements. LRQA offers an optional **threat-modelling workshop** to explore questions such as:

- Which assets need the most protection? (PII, payment data, operational systems)
- Who might target them? (known threat actors, malicious insiders)
- What would a successful breach cost? (regulatory fines, reputational damage)
- Which regulations drive our priorities? (PCI DSS, GDPR, DORA)

When conducted, this workshop underpins a **security assessment framework** that aligns scoping, success criteria and reporting to your business context. For standard engagements, the same inputs are captured via a concise scoping questionnaire and advisory call, ensuring every test targets the highest-value risks before tooling and tactics are chosen.

Threat-modelling workshop (optional)

A facilitated session that builds your security assessment framework – a prioritised attack-path inventory, clear success criteria and a roadmap for testing and remediation.

Choosing the right penetration test

Selecting a penetration test is not a one-size-fits-all exercise. The starting viewpoint, the target environment and the success criteria must all align with business risk and regulatory drivers. This section shows how those elements connect so every engagement delivers usable insight.

Where does the tester begin? Black, grey or white

	Black box	Grey box	White box
Knowledge Sharing	No information about the target system provided, other than the IP addresses or URLs in scope.	Some information about the target environment provided, such as documentation, technologies in use and architecture.	Full knowledge of the target system, including source code, dependencies, design documentation and user documentation.
Focus	External behaviour – vulnerabilities that could be exploited by an external attacker without prior knowledge.	External and internal behaviour – identifying vulnerabilities using knowledge of the system's architecture.	Internal behaviour – logic, code structure and implementation.
Benefits	Mimics an attacker with no inside information, ensuring security flaws are found using the methods of a legitimate external threat actor.	More comprehensive and provides greater assurance than a black box test, without time-consuming decomposition of the environment.	Highly comprehensive and much greater assurance allows for identification of vulnerabilities that may otherwise be difficult to detect.
Examples	Security testing of a banking application from an external perspective.	Testing the security of a backend API, with network access and documentation provided.	Threat modelling and source code review performed throughout the lifecycle of a software development project.

Choosing the right penetration test

Which part of your estate do you need to test?

LRQA delivers a range of penetration testing services, each aimed at a specific attack surface or compliance need. Use the table below to match your security question to the test that answers it – then scope the engagement around the risks that matter most.

LRQA penetration testing services

Testing category	Primary focus	Insight delivered
Web application penetration testing	Web apps and APIs	Finds business-logic and injection flaws automation misses
Mobile application penetration testing	iOS and Android apps	Identifies insecure storage, transport and reverse-engineering gaps
Infrastructure and network penetration testing	Internal networks and internet-facing assets	Validates segmentation, patching and perimeter hardening; uncovers lateral-movement paths
Cloud penetration testing	AWS, Azure, GCP estates	Exposes privilege creep, exposed storage and container breakouts
Social engineering	Phishing, vishing, onsite	Measures human resilience and incident-response speed
Bug-bounty programme	Crowdsourced testing	Extends coverage between scheduled engagements
Blockchain / smart-contract testing	Solidity and rust contracts	Prevents logic flaws that cannot be patched post launch
IoT testing	Embedded devices and RF	Uncovers hardware and firmware exploits with physical impact
ASV scanning	Quarterly PCI scans	Provides mandatory attestation for ROC/SAQ submissions
Firewall security testing	Rule-base review and exploit attempt	Confirms that policy and implementation match in practice
Active directory security review	AD and Azure AD	Highlights paths to domain dominance before attackers do
Hybrid testing	Multi-stack estates	Blends cloud, application and infrastructure scopes under one narrative
Wireless / Wi-Fi penetration testing	802.11, Bluetooth and Zigbee	Demonstrates on-site attack vectors that bypass the perimeter

Choosing the right penetration test

Working with LRQA – four steps to a risk-led test

Collaborate with LRQA through these four, focussed steps to ensure your penetration test targets the risks that matter most. This guided process ensures every engagement is purposeful, measurable and repeatable – turning a single penetration test into lasting security improvement.

1 Business risk

We partner with your team to understand threats against your IT environment, business objectives and desired outcomes

2 Scope prioritisation

Using that threat context, we identify the critical systems and assets that should be in scope

3 Approach determination

We select the right testing style – black-box, grey-box or white-box – and the specific test types to match your risk profile

4 Success criteria

Together we agree on exploitation goals, report format and retest timing so everyone understands when the engagement is complete

Preparing and scoping your penetration test – a risk-led approach

A penetration test pays dividends only when the scope mirrors your real-world risk. Too broad and time is wasted on low-value targets; too narrow and attackers will still find a path you never examined. LRQA therefore begins every engagement with a short, structured scoping exercise that aligns the test with business priorities, compliance duties and operational realities.

Define the scope – start with what matters

First, we identify the 'crown-jewel' assets that would cause the most harm if compromised: customer-data stores, payment platforms, safety-critical OT or shareholder-sensitive IP. We then map likely attack surfaces – cloud control planes, single sign-on, CI/CD pipelines, third-party APIs – and decide which combinations will give the clearest picture of risk. By agreeing these boundaries up front, we avoid the common trap of spending days on legacy systems that attackers would bypass in minutes.

Pre-engagement checklist – questions we answer together

Focus area	Why it matters
Are clear objectives recorded?	Ensures the test answers a defined business or compliance question
Is an authorised point of contact named?	Speeds decision-making if live issues arise
Are legal approvals and NDAs signed?	Protects both parties and meets data-protection law
Is a change-freeze window agreed?	Prevents mid-test configuration shifts that could invalidate results
Is the evidence format confirmed?	Guarantees the final report speaks to boards, engineers and auditors alike
Is a retest window booked?	Locks in a date to prove that fixes actually work

Preparing and scoping your penetration test – a risk-led approach

Budgeting and quick wins

Rigour does not always mean high cost. External perimeter testing combined with an active directory review often uncovers exploitable paths fast, providing a rapid return on effort. Where budgets are tighter, LRQA recommends an initial grey box test focused on your highest-value application or cloud tenancy; findings from that sprint inform a phased roadmap for deeper testing over the next budget cycle.

The hand-off to testing

Once objectives, scope and logistics are locked, LRQA's seven-phase methodology takes over – from reconnaissance through exploitation to remediation and retest. The next section walks through that life-cycle step by step, so you know exactly what 'good' looks like in practice.

From engagement to remediation – what good looks like

A penetration test delivers value only when it follows a disciplined, end-to-end track.
LRQA's seven-phase framework turns raw findings into verified fixes and measurable risk reduction.

Phase		What we do	Key outputs
1	Reconnaissance and enumeration	Harvest open-source intelligence, probe live services, enumerate users and hosts without raising alarms	Accurate attack-surface map, early indicators of high-value targets
2	Mapping and service identification	Group discoveries into external, internal, cloud, identity and application pathways	Visual pathways showing how isolated weaknesses can be chained
3	Vulnerability analysis	Validate vulnerabilities, remove false positives and rank by potential business impact	Prioritised target list so exploitation time is spent where it counts
4	Service exploitation	Launch controlled attacks to prove real-world impact – data access, privilege gain, lateral movement	Concrete evidence – screenshots, logs, proof-of-concept code
5	Pivoting and post-exploitation	From the foothold, explore further routes: credential replay, network traversal, data exfiltration	End-to-end breach scenarios that demonstrate attacker reach
6	Reporting and debrief	Deliver a clear, risk-ranked report and hold an interactive walkthrough that sets remediation priorities	Executive summary, technical detail, remediation plan, risk heat-map
7	Retest and resilience review	After fixes, rerun targeted exploits to confirm closure and capture lessons learned	Verified closure report, lessons learned log, updated threat model

From engagement to remediation – what good looks like

LRQA's seven-phase framework stays the same no matter what you test, it's always:

- **Threat modelling**
- **Reconnaissance**
- **Vulnerability analysis**
- **Controlled exploitation**
- **Reporting**
- **Remediation validation**
- **Retesting**

During each test, you can change the tools and data feeds you 'plug into' one or all the stages.

For example, cloud assessments add IAM-graph mapping and container-escape attempts; social-engineering swaps port-scans for persona profiling and click-rate metrics; IoT reviews include hardware teardown and wireless fuzzing; Active Directory checks use graph-analysis tools and domain-specific exploits.

By keeping the process identical but tailoring the instrumentation, every engagement remains consistent, comparable and firmly focused on the unique risks of your environment.

Selecting a high-assurance testing partner – LRQA's credentials

When assessing potential penetration testing suppliers, look beyond cost. You need independent accreditation, certified expertise, sector-proven compliance experience, a disciplined, intelligence-led methodology and local insight. Here's how LRQA meets each criterion:

Industry-leading accreditation and governance

LRQA is the only organisation worldwide to hold the full suite of CREST accreditations across infrastructure, applications and Red Team testing and is a member of the UK Government's NCSC CHECK scheme. Our ISO 9001, ISO 14001 and ISO 27001 certifications ensure every engagement runs under a rigorous quality and information security management system.

Certified technical expertise

Our consultants hold Offensive Security Certified Professional (OSCP) and Expert (OSCE) credentials alongside CREST-authorised qualifications (CCT Inf, CCT App, CRT). All testers undergo full background screening and many publish research or speak at industry events – ensuring the team probing your defences combines deep theory with real-world practice.

LRQA Cyber Labs also publishes regular vulnerability disclosures, original research and open-source tooling, keeping our methods and your defences at the cutting edge.

Selecting a high-assurance testing partner – LRQA's credentials

8.3 Sector-proven compliance experience

With hundreds of PCI DSS, CBEST, TIBER, NIS2 and DORA engagements completed, LRQA supplies auditors with clause-mapped evidence packs, Attack Indicator Reports and clear executive summaries that align exactly with regulatory requirements in finance, energy, critical infrastructure and beyond.

8.4 Disciplined, intelligence-led methodology

Every test follows our seven-phase framework – threat modelling, reconnaissance, mapping, analysis, exploitation, reporting and retest – enriched by our dedicated threat-intelligence team. That structure ensures findings translate into verified risk reduction time and again.

8.5 Local insight, global best practice

LRQA's cybersecurity experts operate in key regions worldwide, bringing global best practice to your local context. Our regional teams understand specific regulations and threat drivers in your market, while centralised quality controls ensure every engagement delivers the same high-assurance results.

Selecting a high-assurance testing partner – LRQA's credentials

LRQA Penetration Testing – at a glance

CREST & CHECK

Accreditation

Complete CREST suite, NCSC CHECK membership plus ISO 9001/27001

Certified

Expert consultants

Team certified OSCP, OSCE and CREST (CCT Inf/App, CRT) specialists

7 Phases

Proven methodology

End-to-end testing – from threat model through to retest – every time

Comprehensive

Broad service portfolio

Web, mobile, infrastructure, cloud, Red Teaming and more

Debriefs

Actionable insight

Live walkthroughs and retests

Selecting a high-assurance testing partner – LRQA's credentials

9. Self-assessment checklist – are you getting real value?

A truly effective penetration testing partnership delivers far more than a compliance report. It uncovers actionable insights, drives remediation and proves controls really work against today's threats.

You can use the checklist below at your own pace to reflect on whether your current provider is delivering depth, rigour and true business impact – or simply ticking boxes.

	Phase	Yes	No
1	A threat-modelling workshop is held before every test to align scope with your key assets and risks	✓	✓
2	The agreed scope covers external perimeter, cloud, authentication and critical business logic	✓	✓
3	Reports include both technical detail and an executive summary with business impact and remediation priorities	✓	✓
4	A live debrief is scheduled immediately after report delivery to review findings and agree next steps	✓	✓
5	A retest window is booked to prove that critical fixes actually work	✓	✓
6	Your provider integrates up-to-date threat intelligence to shape every engagement	✓	✓
7	Testers hold recognised offensive-security and CREST credentials and are fully background checked	✓	✓
8	Findings are clearly mapped to your compliance obligations (PCI DSS, DORA, NIS2 etc.)	✓	✓
9	Findings are prioritised by risk and include realistic, reproducible proof-of-concept exploits	✓	✓

Score

8–10 Yes: You're getting strong, strategic value

5–7 Yes: You have a solid foundation but should address gaps in scope or methodology

0–4 Yes: Consider a scope sanity check, or a new provider to achieve real depth and rigour

Your next steps

1 Review your self-assessment results

Note each ‘No’ and prioritise the most critical gaps

2 Refine your test scope

Update objectives, include any missing attack surfaces and agree clear success criteria

3 Complimentary scope sanity check

Our experts will validate your approach against best practice, threat intelligence and compliance needs

Get in touch →

About LRQA

LRQA is the leading global assurance partner, bringing together decades of unrivalled expertise in assessment, advisory, inspection and cybersecurity services.

Our solutions-based partnerships are supported by data-driven insights that help our clients solve their biggest business challenges. Operating in more than 150 countries with a team of more than 5,000 people, LRQA's award-winning compliance, supply chain, cybersecurity and ESG specialists help more than 61,000 clients across almost every sector to anticipate, mitigate and manage risk wherever they operate.

In everything we do, we are committed to shaping a better future for our people, our clients, our communities and our planet.

Get in touch

Visit **lrqa.com** for more information or email **enquiries@lrqa.com**

LRQA
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES
United Kingdom