Penetration Testing for Compliance

A short guide to what DORA, NIS2, CyFun, ISO 27001 and NIST actually require, and where insurance and client due diligence fit in

CommSec
CYBER SECURITY

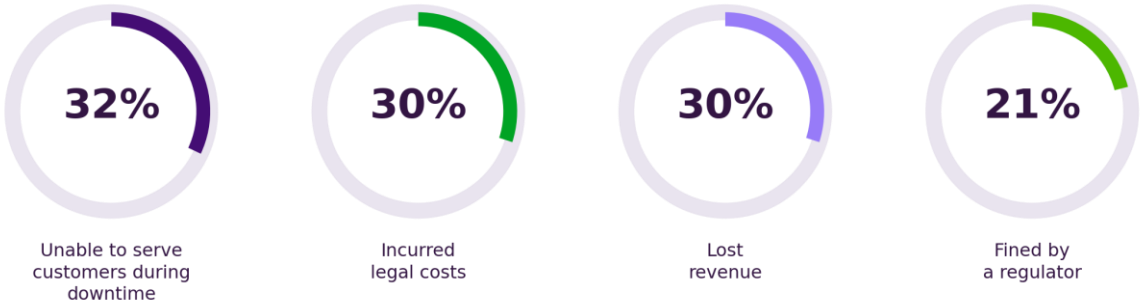
Why compliance now demands proof, not paperwork

Every major cyber security framework is converging on the same underlying question. Not whether an organisation has policies, but whether it can prove its controls work. An organisation can hold every certificate on the wall and still be one unpatched vulnerability away from a breach notification.

The WannaCry outbreak of 2017 remains the clearest illustration. A self-propagating worm exploited a known Windows vulnerability, one Microsoft had already patched two months earlier, and spread to more than 300,000 computers across 150 countries within days. The vulnerability was not a mystery, and the fix already existed. What was missing was any process that would have surfaced the exposure and forced action before an attacker did it instead.

Penetration testing is the mechanism that closes that gap. A vulnerability scan tells an organisation what might be wrong. A penetration test, where a qualified tester attempts to exploit a weakness the way an attacker would, tells them what is genuinely exploitable and what the real business impact would be.

The same pattern holds closer to home. Two-thirds of Irish businesses experienced at least one cyberattack in the last year, and more than a third were hit more than three times (Gallagher/Cebr survey, Irish Times, July 2026). Where an attack caused disruption, the financial and operational fallout was significant.



Impact of cyberattacks on Irish businesses in the last year (Gallagher/Cebr survey, Irish Times, July 2026)

Global figures tell a similar story. Where organisations experienced a cyberattack, the most common consequences were unplanned downtime, a breach of data, and financial loss, and budgets are moving to catch up: US enterprises now spend an average of $187,000 annually on penetration testing, close to 11% of their total IT security budget, with over half of CISOs planning to raise that budget further (Pentera, The State of Pentesting 2025).

How five major frameworks treat testing

Framework	Named or implied	Where it lives	What it asks for
DORA	Named directly	Article 24(2)	Annual testing for all in-scope entities; threat-led penetration testing every three years for higher-risk entities.
NIS2	Implied	Article 21(2)(f)	Policies and procedures to assess the effectiveness of security measures. Regulators read this as requiring adversarial testing, not documentation alone.
CyFun	Named at Essential level	Essential tier control set	Basic level stops at documenting vulnerabilities. Essential level names a testing programme directly, including post-test validation.
ISO 27001:2022	Implied	Risk assessment, control effectiveness, and Annex A technical vulnerability controls	No explicit mandate, but auditors expect testing as evidence that controls work, particularly for internet-facing systems.
NIST	Implied	CSF and SP 800-53 assessment obligations; SP 800-115 methodology	Describes assessment and monitoring obligations, and supplies the technical methodology other frameworks reference.

The split between prescriptive and descriptive frameworks is not an oversight. DORA governs a sector where a breach has an immediate, quantifiable knock-on effect, so its regulators named the control outright. NIS2, ISO 27001 and NIST cover a far wider population of organisations, so they favour proportionate, outcome-based language instead. The frameworks differ in how prescriptive they are willing to be. They do not differ on the underlying expectation: prove your controls hold under attack.

What each framework actually asks for

DORA

Digital operational resilience testing is one of DORA's core pillars. Article 24(2) requires financial entities to use a range of assessments, tests, methodologies, practices and tools to confirm their defences hold up. Every in-scope entity needs at least annual testing. A smaller group of higher-risk entities must also carry out threat-led penetration testing at least every three years.

NIS2

Article 21(2)(f) requires essential and important entities to have policies and procedures to assess the effectiveness of their cyber security risk management measures. The directive never uses the words penetration test, but regulators and ENISA's technical guidance have converged on the same reading: effectiveness of a technical control cannot be demonstrated through documentation alone.

CyFun

Ireland's adopted CyberFundamentals framework is one of two recognised routes to NIS2 conformity. At Basic level, CyFun stops at identifying and documenting vulnerabilities. At Important level, it asks organisations to consider vulnerability scanning. Only at Essential level does it name penetration testing directly, advising organisations to establish a testing programme appropriate to their size and complexity.

ISO 27001:2022

The standard does not explicitly require penetration testing, but it does require organisations to identify technical vulnerabilities, assess control effectiveness, and treat the risks they uncover. For environments with internet-facing systems, web applications, or sensitive data, vulnerability scanning alone rarely satisfies an auditor. Most organisations combine regular scanning with at least annual penetration testing, plus testing after significant change.

NIST

The Cybersecurity Framework and SP 800-53 controls describe assessment and continuous monitoring obligations rather than naming a specific test type. SP 800-115, the Technical Guide to Information Security Testing and Assessment, sets out the methodology that underpins most professional penetration testing, and is frequently referenced by other frameworks, including PCI DSS, when they call for testing to an industry-accepted standard.

Beyond the regulation: insurance and client requirements

Compliance is rarely the only reason a penetration test lands on an IT manager's desk. Two other drivers show up just as often, and the same test report typically serves all three.

Cyber insurance

Insurers increasingly ask for evidence of regular, independent security testing before binding or renewing cover, and a clear pen test report can support a stronger premium or terms. Underwriters are, in effect, asking the same question as a regulator: can you prove your controls work.

Client and supply chain due diligence

Enterprise customers and public sector procurement processes are asking smaller suppliers to evidence their security posture before signing a contract. A current, CREST-accredited penetration test report is one of the fastest ways to satisfy that request, and can shorten a due diligence cycle considerably.

Board and shareholder exposure

The governance stakes are rising too. Most Irish businesses now expect a serious cybercrime incident to trigger legal or shareholder action, and the large majority are aware that company directors can face personal liability after a breach (Gallagher/Cebr survey, Irish Times, July 2026). A penetration test report is one of the clearest ways for a board to evidence that it acted on a known risk rather than ignored it.

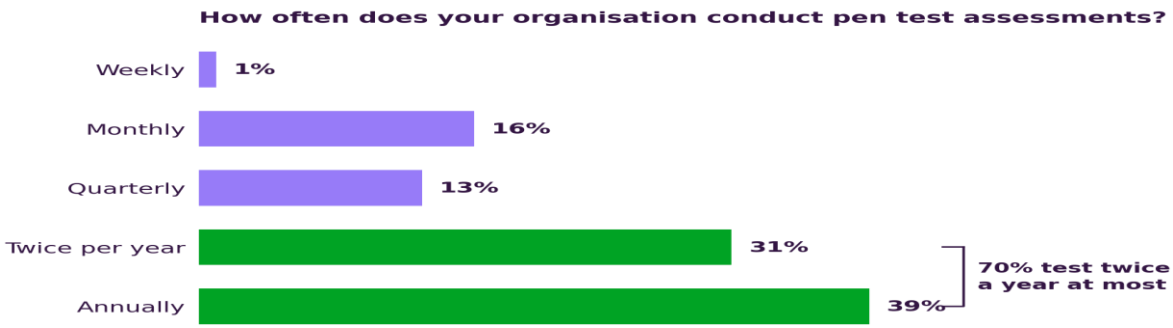
Cyberattack frequency and governance exposure for Irish businesses (Gallagher/Cebr survey, Irish Times, July 2026)

Sector-specific and public sector requirements

Beyond the frameworks above, individual sectors and public bodies increasingly build cyber security evidence directly into their own review and procurement processes. Education providers reviewed under QQI's CINNTE cyclical review process, for example, are assessed against QQI's statutory quality assurance guidelines, which state that industry standard cybersecurity measures should be in place on core online platforms to protect learner data. Public sector bodies work to the National Cyber Security Centre's Public Service Cyber Security Baseline Standards, a NIST-aligned framework built around the same identify, protect, detect, respond and recover themes as the frameworks above. Where an organisation sits inside one of these sectors, a penetration test report is often the fastest way to evidence the relevant control.

Building a testing cadence

Most organisations are not testing anywhere near the cadence the frameworks above expect. In a 2025 global survey, 70% of organisations tested no more than twice a year, and annual testing was still the single most common answer (Pentera, The State of Pentesting 2025).



How often organisations conduct penetration test assessments (Pentera, The State of Pentesting 2025)

- Do not wait for a specific clause number before scheduling a test.
- Test at minimum annually, and more frequently for critical systems or after significant change.
- Map findings explicitly to the controls or framework clauses they evidence.
- Retest after remediation. An unresolved finding sitting in a report is proof a weakness was identified and not acted on.
- Keep the report accessible for audits, insurance renewal, and client due diligence, not filed away unread.

How CommSec approaches penetration testing for compliance

CommSec's penetration testing team is made up of CREST accredited consultants, and CommSec is itself an ISO 27001 certified organisation. Testing is manual-led rather than automated, going beyond a vulnerability scan to find and fix the weaknesses that matter.

- CREST certified pen testers, using leading-edge tools with expert manual validation.
- Every engagement scoped properly to your environment and business objectives.
- Clear, high quality reporting that maps findings to the frameworks it evidences, for auditors, insurers, and clients alike.
- Retests encouraged after remediation, to confirm fixes and keep the audit trail current.
- Competitive, transparent rates, with a free consultation to scope the right test for your organisation.

What a retest actually involves

A retest is not included as standard, but we encourage clients to book one once remediation work is complete. Because a retest focuses only on the high and critical risk findings from the original engagement, rather than repeating the full scope, it typically takes just a day or two for a standard engagement. That keeps the cost and time proportionate, while still giving auditors, insurers, and clients current evidence that the weaknesses identified were genuinely fixed.

Whether the driver is NIS2 transposition, a DORA obligation, an ISO 27001 renewal, a cyber insurance requirement, or a client's due diligence questionnaire, the practical takeaway is the same: build a testing cadence now, rather than waiting to be told the exact clause number that demands it.

Managed Vulnerability Scanning & Assessment

Between full penetration tests, CheckScan+ keeps you covered. Our managed vulnerability scanning service runs regular scans, prioritises findings by real-world risk, and includes expert review of the results. It supports NIS2, DORA, and ISO 27001 compliance alignment, reduces the operational burden on your team, and gives you continuous visibility rather than a single annual snapshot.

Book a free consultation

Speak with our CREST certified testers about scoping a penetration test for your compliance, insurance, or client requirements.

commsec.ie/contact | +353 1 536 7320