rasotec

FREE REFERENCE SHEET

ISO/IEC 27001:2022 and Penetration Testing

Which controls a pentest can provide evidence for, and what the standard does not require

ISO/IEC 27001:2022 does not prescribe penetration testing as a standalone requirement. A pentest can, however, provide evidence for several controls, but only to the extent that its scope, objectives and methodology actually address the control. ISO/IEC 27002:2022 serves as implementation guidance for the Annex A controls.

Control	Topic	What a penetration test can show	Relation
Directly related to security testing			
A.8.8	Management of technical vulnerabilities	Whether vulnerabilities are exploitable, how weaknesses combine into attack paths, whether compensating controls work, and whether fixes hold in a retest	Direct
A.8.29	Security testing in development and acceptance	Testing of new applications, APIs, major releases and security-sensitive functions before they are accepted into production	Direct
ISMS clauses and governance			
Clause 6.1.3	Information security risk treatment	Once pentesting is selected as a risk treatment and recorded in the Statement of Applicability, it must be carried out as defined	Supporting
Clause 9.1	Monitoring, measurement, analysis and evaluation	Metrics such as critical findings remediated within the defined time or fixes verified by retest	Supporting
A.5.35	Independent review of information security	Independent technical evidence; it does not replace the broader independent review	Supporting
A.5.36	Compliance with policies, rules and standards	Reports, schedules and retests prove that your own pentest policy is followed	Supporting
Technical controls			
A.8.9	Configuration management	Whether exposed services, default credentials, excessive permissions or insecure cloud settings can actually be exploited	Supporting
A.8.20	Network security	Whether firewall rules, routing, VPN and remote access controls hold against realistic attack paths	Supporting
A.8.22	Segregation of networks	Whether network boundaries prevent access between zones, e.g. in an assumed-breach test	Supporting
A.8.31	Separation of development, test and production	Whether an attacker can cross environments via shared credentials, IAM, CI/CD or network paths	Supporting
A.8.32	Change management	Targeted tests of significant changes: new authentication, cloud migration, newly exposed applications, new segmentation	Supporting
A.8.34	Protection of systems during audit testing	Governs how the test is run: authorization, scope, exclusions, test windows, rules of engagement and escalation contacts	Supporting
A.5.23	Information security for use of cloud services	Testing of cloud components within your responsibility and the provider's testing policy	Supporting

Control	Topic	What a penetration test can show	Relation
Secure development			
A.8.25	Secure development life cycle	Pentests as one assurance activity next to threat modeling, code review and automated analysis	Supporting
A.8.26	Application security requirements	Test cases that verify requirements, e.g. that tenant A cannot access objects of tenant B	Supporting
A.8.28	Secure coding	Exploitable coding flaws such as injection, XSS, SSRF, path traversal and authorization flaws	Supporting
A.8.30	Outsourced development	Independent evidence about the security of software delivered by suppliers	Supporting
Threat intelligence, detection and incident response			
A.5.7	Threat intelligence	Input for realistic test scenarios and priorities; the test itself does not satisfy A.5.7	Supporting
A.8.16	Monitoring activities	Whether simulated attack activity generates telemetry, triggers alerts and is investigated	Exercise
A.5.24–A.5.27	Incident management: planning, assessment, response, learning	Assumed-breach, adversary-simulation, purple-team or tabletop exercises rather than a conventional pentest	Exercise

Direct control relates directly to security testing · Supporting a suitably scoped pentest can provide evidence · Exercise requires an attack simulation or incident-response exercise

What ISO/IEC 27001:2022 does not require

- [ ] An external penetration test once per year
- [ ] A pentest for every application or release
- [ ] A specific tester certification, e.g. CREST
- [ ] That the test must be external, or that a vulnerability scan is always insufficient

Such requirements can still come from your risk treatment, policies, contracts, customers or regulation.

Three questions for every control

- [ ] **Does the control apply?** Decided by your ISMS and risk treatment.
- [ ] **Is a pentest the right way to test it?** Depends on the control, system and risk.
- [ ] **Does the test prove effectiveness?** Only if scope, method and evidence address the control.

Planning your ISO 27001 pentest program?

We help you scope penetration tests around the controls you need evidence for. Full article: **Penetration testing and ISO/IEC 27001**

Book a free 30-minute consultation · **contact@rasotec.com** · **www.rasotec.com**