ISO/IEC 27001:2022

Pentesting Requirements

A practical guide for IT leaders, CISOs, and security teams navigating ISO 27001:2022 certification - with specific Annex A control references, pentest mapping, and 2022 revision highlights across all 93 controls.

Contents

01 Quick Summary

WHAT CISOS AND IT LEADERS NEED TO KNOW

ISO/IEC 27001:2022 is the world's leading standard for Information Security Management Systems (ISMS). It does not use the words 'penetration testing' as an explicit mandate - but no serious Stage 2 certification audit passes without one. Penetration testing is the primary technical evidence that Annex A controls are operating effectively, not just documented. Here is the simplified version:

AT A GLANCE

- Penetration testing directly satisfies A.8.8 (Technical Vulnerability Management) and A.8.29 (Security Testing in Development) - the two core pentest controls.
- Clause 9.1 (Monitoring, Measurement, Analysis and Evaluation) requires measurable evidence of control effectiveness - pentests deliver this.
- ISO 27001:2022 restructured Annex A from 114 controls (14 domains) to 93 controls (4 themes): Organizational, People, Physical, and Technological.
- 11 new controls were added in 2022, including A.5.7 (Threat Intelligence), A.5.23 (Cloud Security), and A.8.16 (Monitoring Activities).
- Both internal and external attack surfaces must be tested - scope follows the ISMS boundary.
- Annual penetration testing is the expected cadence for certification maintenance.
- Vulnerability scanning alone does not satisfy A.8.8 - active exploitation validation is expected.
- Retesting after remediation is required before surveillance audits.

02 What Is ISO 27001:2022?

BACKGROUND AND CONTEXT

ISO/IEC 27001:2022 is an international standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It specifies the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). It is the most widely adopted information security certification globally, with over 70,000 certified organizations worldwide.

Who Needs ISO 27001?	Examples
SaaS and cloud providers	Any software company handling customer data - increasingly required by enterprise procurement
Financial services firms	Banks, fintechs, insurance companies processing sensitive financial and personal data
Healthcare and life sciences	Alongside HIPAA (US) - ISO 27001 often required by EU and global healthcare clients

Government contractors	Many procurement frameworks require ISO 27001 or equivalent for sensitive government contracts
Supply chain participants	Vendors in regulated supply chains (automotive: TISAX, aerospace, defense) often required to certify
Managed service providers	MSPs handling client infrastructure increasingly expected to hold ISO 27001 by enterprise clients

Key Terms

Term	Plain English Meaning
ISMS	Information Security Management System - the governance framework defined by ISO 27001.
Annex A	The 93 reference controls organizations select from based on their risk assessment.
SoA	Statement of Applicability - documents which Annex A controls apply, which are excluded, and why.
Stage 1 Audit	Documentation review - auditor confirms ISMS documentation is in order before Stage 2.
Stage 2 Audit	On-site evidence review - auditor checks that controls are implemented and operating effectively. This is where pentesting evidence is examined.
Surveillance Audit	Annual check between recertification cycles - evidence of continued control operation required.
Recertification Audit	Full audit every 3 years - ISMS must demonstrate sustained effectiveness.
Nonconformity	A finding where a control is not implemented or not operating as required. Major NCs can block certification.
ISO 27002:2022	The companion implementation guidance standard for Annex A controls - auditors reference it.

03 The ISMS Structure: Clauses and Annex A

UNDERSTANDING THE TWO-LAYER FRAMEWORK

ISO 27001 follows the Harmonized Structure (formerly Annex SL) shared by ISO 42001, ISO 9001, and other management system standards. This means it has two layers: mandatory governance clauses (4-10) and Annex A reference controls selected based on risk assessment.

Layer	What It Covers
Clauses 4-10 (Mandatory)	Context of the organization, leadership, planning (risk assessment and treatment), support, operations, performance evaluation (Clause 9.1 - key pentest hook), and improvement. All mandatory.

Annex A Controls (Risk-Based)	93 reference controls across 4 themes. Selected via Statement of Applicability based on risk assessment. Auditors review the SoA to confirm appropriate controls are selected and implemented.
ISO 27002:2022 (Guidance)	Non-normative implementation guidance for each Annex A control. Auditors use ISO 27002 to assess the quality of control implementation - it is the 'how' behind the Annex A 'what'.

The 4 Annex A Control Themes (ISO 27001:2022)

Theme	Controls	Key Security Areas
A.5 - Organizational	37 controls (A.5.1-A.5.37)	Policies, threat intelligence, access control policy, supplier security, incident management, compliance, information classification
A.6 - People	8 controls (A.6.1-A.6.8)	Screening, employment terms, training and awareness, discipline, offboarding, remote working, security reporting
A.7 - Physical	14 controls (A.7.1-A.7.14)	Physical security perimeters, entry controls, equipment security, clear desk, secure disposal, cabling security
A.8 - Technological	34 controls (A.8.1-A.8.34)	Endpoint protection, privileged access, encryption, logging, vulnerability management, security testing, network security, cloud security, secure development

CLAUSE 9.1 - THE MEASUREMENT MANDATE

Clause 9.1 (Monitoring, Measurement, Analysis and Evaluation) requires organizations to determine what needs to be monitored, what methods will be used, when analysis occurs, and who is responsible. It demands objective evidence that security controls are actually working. Penetration testing is the strongest form of evidence available for Clause 9.1 - it demonstrates not just that a control exists, but that it holds up under real-world attack conditions. Auditors treat Clause 9.1 as the bridge between documented controls and demonstrated effectiveness.

04 Required Controls and Pentest Mapping

ISO 27001:2022 ANNEX A CONTROLS WITH SECURITY TESTING RELEVANCE

The controls below are drawn directly from ISO/IEC 27001:2022 Annex A. While the standard does not mandate penetration testing by name, the controls listed here are the ones certification auditors look to for pentest evidence. Controls are listed with their 2022 numbering alongside legacy 2013 references for organizations in transition.

Organizational Controls - A.5 (Key Pentest-Relevant Controls)

Annex A Control	Control Name	Pentest Relevance
A.5.7 (NEW)	Threat Intelligence	Threat intelligence gathering directly informs pentest scope. Pentest findings are a primary source of operational threat intelligence - real exploitability data, not theoretical advisories.
A.5.20	Addressing Security Within Supplier Agreements	Third-party security testing validates supplier controls. Requires that security requirements are verifiable - pentesting supplier-facing systems or APIs confirms requirements are met in practice.
A.5.21	Managing Information Security in the ICT Supply Chain	Supply chain security testing validates that third-party components (APIs, SDKs, open source libraries) do not introduce exploitable vulnerabilities into the ISMS boundary.
A.5.23 (NEW)	Information Security for Use of Cloud Services	Cloud configuration review and exploitation testing validates that cloud service security controls meet ISMS requirements. AWS/Azure/GCP misconfigurations are in scope.
A.5.25	Assessment and Decision on Information Security Events	Pentest events generate information security events that must be assessed. Tests whether the assessment and decision process actually operates correctly.
A.5.36	Compliance with Policies, Rules and Standards for Information Security	Penetration testing provides technical evidence of compliance with implemented controls. Nonconformities found in pentests must be addressed under this control.

Technological Controls - A.8 (Core Pentest Controls)

The Technological theme contains the controls most directly satisfied by penetration testing. A.8.8 and A.8.29 are the two controls auditors specifically reference when asking for pentest evidence.

Annex A Control	Control Name	Pentest Relevance
A.8.8	Management of Technical Vulnerabilities	THE PRIMARY PENTEST CONTROL. Requires timely identification and evaluation of technical vulnerabilities and appropriate action. Penetration testing is the gold standard for satisfying this control - it goes beyond scanning to validate exploitability.
A.8.29	Security Testing in Development and Acceptance	THE DEVELOPMENT PENTEST CONTROL. Requires security testing processes defined and performed throughout the development lifecycle. Web application pentests and pre-release security testing satisfy this control directly.
A.8.2	Privileged Access Rights	Privilege escalation testing validates that privileged access is properly restricted. Testers attempt to gain admin rights through misconfiguration, credential abuse, or application flaws.

A.8.3	Information Access Restriction	Access control testing - IDOR, broken authorization, API access bypass - validates that access restrictions are enforced technically, not just in policy.
A.8.5	Secure Authentication	Authentication testing covers MFA bypass, password policy enforcement, brute force resistance, SSO weaknesses, and session management vulnerabilities.
A.8.9 (NEW)	Configuration Management	Configuration review and hardening validation tests that systems are deployed with secure baselines - common findings include default credentials, unnecessary services, and insecure defaults.
A.8.11 (NEW)	Data Masking	Testing validates that sensitive data is appropriately masked in non-production environments - development/staging data exposure is a common pentest finding.
A.8.12 (NEW)	Data Leakage Prevention	Pentest validates DLP controls - tests whether sensitive data can be exfiltrated via email, USB, cloud uploads, or API responses without triggering controls.
A.8.15	Logging	Pentest validates that logging captures attack activity - if a pentest generates no alerts or log entries, that is a direct A.8.15 / Clause 9.1 finding.
A.8.16 (NEW)	Monitoring Activities	Pentest exercises validate whether monitoring systems detect adversarial activity. Red team exercises are particularly relevant - if detection fails during testing, it will fail during real attacks.
A.8.20	Networks Security	External and internal network pentests validate firewall rules, DMZ architecture, service exposure, and network boundary protections.
A.8.22	Segregation of Networks	Network segmentation testing validates that VLAN boundaries hold, lateral movement between segments is blocked, and critical systems are isolated from less-trusted environments.
A.8.24	Use of Cryptography	Encryption testing validates TLS configuration, cipher suite strength, certificate management, and key storage - weak cryptography is a common high-severity pentest finding.
A.8.25	Secure Development Life Cycle	Security testing is a required component of the SDLC. Pentest provides evidence that the SDLC produces secure outputs at each stage.
A.8.26	Application Security Requirements	Web application and API pentesting validates that defined security requirements are actually implemented - authentication, authorization, input validation, and data protection.

A.8.28	Secure Coding	Penetration testing identifies vulnerabilities resulting from insecure coding - SQL injection, XSS, insecure deserialization - that SAST/DAST may miss.
A.8.31	Separation of Development, Test and Production Environments	Environment isolation testing validates that production credentials, data, and systems are not accessible from development or test environments.
A.8.34 (NEW)	Protection of Information Systems During Audit Testing	Rules of engagement and testing safeguards ensure that the pentest itself does not cause a production incident. Proper scoping and controls protect systems during testing.

A.8.8 - THE CORE PENTEST CONTROL (ISO 27002 GUIDANCE)

ISO 27002:2022 guidance for A.8.8 explicitly states that organizations should:

- 'Perform periodic, documented penetration tests, either by internal staff or by an authenticated third-party.'
- Subscribe to vulnerability alerts and assess exposure to published vulnerabilities.
- Maintain an asset inventory to identify what needs to be assessed.
- Implement remediation within defined timeframes based on risk rating.

This is the closest ISO 27001 gets to a direct penetration testing requirement. Certification auditors treat a documented annual pentest with remediation evidence as the minimum bar for A.8.8.

05

Highlighted Control Areas

SECURITY TOPICS WITH SPECIFIC ANNEX A MAPPINGS

The following areas represent the most pentest-relevant control categories in ISO 27001:2022. Each maps to specific Annex A controls and includes guidance on what security testing should validate.

Password Hygiene and Credential Security

RELEVANT CONTROLS: A.8.5, A.5.16, A.8.2

A.8.5 (Secure Authentication) requires authentication controls appropriate to the risk of unauthorized access. A.5.16 (Identity Management) governs the identity lifecycle. A.8.2 (Privileged Access Rights) specifically addresses high-privilege credential management. ISO 27002 guidance for A.8.5 recommends multi-factor authentication, strong password policies, password managers, and controls against brute force and credential stuffing attacks.

Testing Area	Annex A Control
Password complexity, length, and lockout policy enforcement	A.8.5 - Secure Authentication
Multi-factor authentication implementation and bypass testing	A.8.5 - (MFA explicitly recommended in ISO 27002 guidance)

Default credentials on systems, applications, and network devices	A.8.5, A.8.9 - Configuration Management
Privileged account credential security and management	A.8.2 - Privileged Access Rights
Service account and API key management	A.8.2, A.5.16 - Identity Management
Password reset and credential recovery workflow testing	A.8.5 - authentication resilience
Credential exposure in code repositories, logs, or error messages	A.8.28 - Secure Coding; A.8.11 - Data Masking

Access Management

RELEVANT CONTROLS: A.5.15, A.5.16, A.5.18, A.8.2, A.8.3

Access management is one of the most tested areas in ISO 27001 audits. A.5.15 (Access Control) establishes the policy foundation. A.8.3 (Information Access Restriction) requires technical enforcement. A.8.2 (Privileged Access Rights) demands that elevated access is strictly controlled and reviewed. The principle of least privilege must be demonstrated in practice through testing, not just declared in policy.

Testing Area	Annex A Control
Role-based access control and least privilege enforcement	A.5.15 - Access Control; A.8.3 - Information Access Restriction
Privilege escalation - vertical (user to admin) and horizontal (user to user)	A.8.2 - Privileged Access Rights; A.8.3
Broken object-level authorization (IDOR/BOLA) in applications and APIs	A.8.3 - Information Access Restriction; A.8.26
Orphaned accounts - terminated employees, unused service accounts	A.5.18 - Access Rights; A.6.5 - Responsibilities After Termination
Admin interface exposure and hardening	A.8.2, A.8.9 - Configuration Management
Third-party and supplier access validation	A.5.20 - Supplier Agreements; A.5.21 - ICT Supply Chain

Vulnerability Management

RELEVANT CONTROLS: A.8.8 (PRIMARY), A.8.9, A.5.7

A.8.8 is the definitive vulnerability management control in ISO 27001:2022. ISO 27002 guidance explicitly calls for periodic penetration testing as part of A.8.8 implementation. A.5.7 (Threat Intelligence) feeds threat data into vulnerability prioritization. A.8.9 (Configuration Management) addresses hardening gaps. Vulnerability scanning and penetration testing are complementary - scanning identifies known CVEs, pentesting validates whether they are actually exploitable in your specific environment.

Activity	Annex A Control / Cadence
Vulnerability scanning - automated, continuous or periodic	A.8.8 - Management of Technical Vulnerabilities
Annual penetration test - external and internal	A.8.8 - explicitly referenced in ISO 27002 implementation guidance
Web application and API security testing	A.8.29 - Security Testing in Development and Acceptance
Cloud configuration review and exploitation testing	A.5.23 - Cloud Security; A.8.8
Patch management timeline validation	A.8.8 - timely remediation per risk rating
Post-change security testing (after significant changes)	A.8.8 - re-evaluate after environmental changes
Remediation retesting before surveillance audit	A.8.8, Clause 9.1 - demonstrating control effectiveness

Network Segmentation and Security

RELEVANT CONTROLS: A.8.20, A.8.22, A.8.21

A.8.22 (Segregation of Networks) explicitly requires that networks be segregated based on information sensitivity and system criticality. A.8.20 (Networks Security) governs the broader network security controls. A.8.21 (Security of Network Services) covers the security of services delivered over networks. Network segmentation testing is one of the most valuable pentest activities for ISO 27001 - it validates that logical and physical boundaries actually prevent lateral movement between trust zones.

Testing Area	Annex A Control
Network segmentation - VLAN boundary testing and lateral movement	A.8.22 - Segregation of Networks
Firewall rule review and bypass attempts	A.8.20 - Networks Security
DMZ architecture validation - can DMZ hosts reach internal systems?	A.8.22, A.8.20
Production vs. development/test environment isolation	A.8.31 - Separation of Development, Test and Production
Guest network isolation from corporate systems	A.8.22 - Segregation of Networks
Cloud VPC, security group, and subnet configuration testing	A.5.23 - Cloud Services; A.8.22
Network service exposure - unnecessary ports and services	A.8.20, A.8.9 - Configuration Management

Encryption and Cryptography

RELEVANT CONTROLS: A.8.24, A.8.26, A.5.33

A.8.24 (Use of Cryptography) is the primary encryption control. It requires a policy on cryptographic controls and key management. ISO 27002 guidance references NIST, ENISA, and FIPS standards for approved algorithm selection. A.5.33 (Protection of Cryptographic Keys) governs key lifecycle management. Penetration testing validates that encryption is correctly implemented - not just that a policy exists. Weak cipher suites, expired certificates, and cleartext data transmission are common high-severity findings.

Testing Area	Annex A Control
TLS/SSL configuration - cipher suites, protocol versions, certificate validity	A.8.24 - Use of Cryptography
Cleartext data transmission detection - internal and external	A.8.24, A.8.26 - Application Security Requirements
Sensitive data exposure in API responses and error messages	A.8.11 - Data Masking; A.8.26
Encryption key storage and exposure testing	A.5.33 - Protection of Cryptographic Keys
Database encryption validation at rest	A.8.24 - cryptographic controls
Hardcoded secrets in source code or configuration files	A.8.28 - Secure Coding; A.5.33
Certificate management and rotation procedures	A.8.24, A.8.9 - Configuration Management

Data Segregation and Classification

RELEVANT CONTROLS: A.5.12, A.5.13, A.8.10, A.8.11

A.5.12 (Classification of Information) and A.5.13 (Labelling of Information) establish the data classification framework. A.8.10 (Information Deletion) and A.8.11 (Data Masking) are new 2022 controls that address data lifecycle and protection in operational environments. Penetration testing validates that classification controls are enforced technically - not just labeled in policy. Multi-tenant SaaS environments and shared databases are high-risk areas for data segregation failures.

Testing Area	Annex A Control
Multi-tenant data isolation - can Tenant A access Tenant B data?	A.5.12, A.8.3 - Information Access Restriction
Data classification enforcement in API responses	A.5.12, A.8.11 - Data Masking
Non-production environment data masking validation	A.8.11 - Data Masking (new 2022 control)
Database access control - unauthorized queries to sensitive tables	A.8.3, A.8.10 - Information Deletion
Data leakage via logs, error messages, or cache headers	A.8.12 - Data Leakage Prevention (new 2022)
Storage bucket and file share access control testing	A.5.12, A.5.23 - Cloud Security

Third-Party and Supply Chain Security

RELEVANT CONTROLS: A.5.19, A.5.20, A.5.21, A.5.22, A.5.23

ISO 27001:2022 significantly strengthened supplier security controls. A.5.21 (ICT Supply Chain) is an expanded control addressing software supply chain risks - directly relevant after high-profile supply chain attacks. A.5.23 (Cloud Security) is a brand new 2022 control for cloud service provider security. Supply chain testing validates that third-party components - APIs, SDKs, open source libraries, cloud services - do not introduce exploitable vulnerabilities into the ISMS boundary.

Testing Area	Annex A Control
Third-party API security testing	A.5.20 - Supplier Agreements; A.5.23 - Cloud Security
Software composition analysis (SCA) of dependencies	A.5.21 - ICT Supply Chain; A.8.8
Cloud service configuration review and exploitation testing	A.5.23 - Cloud Security (new 2022 control)
Supplier access path testing - VPNs, portals, shared credentials	A.5.19 - Supplier Relationships; A.8.2
Vendor-provided component security assessment	A.5.21 - ICT Supply Chain
Penetration testing firm's own ISO 27001 certification	A.5.19 - due diligence on security service providers

Logging, Monitoring and Detection Validation

RELEVANT CONTROLS: A.8.15, A.8.16, A.5.25, A.5.26

A.8.15 (Logging) and A.8.16 (Monitoring Activities - new 2022) together require that organizations generate, protect, and actively monitor security logs. A.8.16 explicitly lists penetration testing as a method for extending security monitoring to establish system baselines. If a penetration test runs simulated attacks and no SIEM alerts fire, no logs are generated, or no incident response is triggered - that is a direct A.8.15/A.8.16 finding.

Testing Area	Annex A Control
SIEM/IDS detection validation - did pentest activity generate alerts?	A.8.16 - Monitoring Activities (new 2022)
Log completeness - are all access and security events captured?	A.8.15 - Logging
Log integrity - can logs be tampered with or deleted?	A.8.15 - Logging protection
Log retention validation - are logs available for the required period?	A.8.15 - retention requirements
Incident response trigger testing - do IR procedures activate?	A.5.26 - Response to Information Security Incidents

Audit trail bypass testing - can logging be disabled during attack?	A.8.15, A.8.16

06 ISO 27001:2013 vs. 2022: What Changed?

KEY CHANGES AFFECTING PENTEST PROGRAMS

Organizations certified to ISO 27001:2013 had until October 31, 2025 to transition to the 2022 version. The 2022 revision significantly reorganized Annex A and added 11 new controls relevant to modern security testing programs.

Aspect	ISO 27001:2013	ISO 27001:2022
Control structure	114 controls across 14 domains	93 controls across 4 themes
Primary pentest control	A.12.6.1 - Technical Vulnerability Management	A.8.8 - Management of Technical Vulnerabilities (expanded)
Development security testing	A.14.2.8 + A.14.2.9 (separate controls)	A.8.29 - Security Testing in Development (merged and strengthened)
Cloud security	Not explicitly addressed	A.5.23 - Information Security for Use of Cloud Services (new)
Threat intelligence	Not explicitly required	A.5.7 - Threat Intelligence (new)
Monitoring activities	A.12.4 - Logging and Monitoring	A.8.16 - Monitoring Activities (expanded, explicitly references pentesting)
Data masking	Not explicitly addressed	A.8.11 - Data Masking (new)
Data leakage prevention	Not explicitly addressed	A.8.12 - Data Leakage Prevention (new)
Configuration management	Addressed via A.12	A.8.9 - Configuration Management (new, explicit control)
Supply chain security	A.15 - Supplier Relationships	A.5.19-A.5.22 + A.5.23 (significantly expanded)

TRANSITION DEADLINE PASSED: ALL ORGANIZATIONS NOW NEED 2022

The ISO 27001:2013 to 2022 transition deadline was October 31, 2025. All active certificates issued under the 2013 version have expired or been reissued under the 2022 standard. If your pentest program still maps findings to 2013 Annex A control numbers, update your reporting templates to reference 2022 control numbers (e.g., A.12.6.1 to A.8.8; A.14.2.8/9 to A.8.29). Auditors at surveillance and recertification audits will reference the 2022 controls exclusively.

07 Pentest Scope for ISO 27001

WHAT SHOULD BE IN SCOPE?

ISO 27001 pentest scope is defined by the ISMS boundary - the systems, services, locations, and processes included in the certified scope. In practice, any component that stores, processes, or transmits information assets covered by the ISMS should be considered. The Statement of Applicability (SoA) defines which controls apply, and pentest scope should cover the systems those controls protect.

Component	Typical Testing Focus	Relevant Controls
External perimeter	Public-facing assets, IP ranges, DNS, exposed services, boundary controls	A.8.20, A.8.8
Web applications and APIs	Authentication, authorization, business logic, injection, OWASP Top 10	A.8.26, A.8.29, A.8.3
Internal network	Segmentation, lateral movement, inter-VLAN access, internal service exposure	A.8.22, A.8.20
Cloud infrastructure	AWS/Azure/GCP IAM, storage, misconfigurations, cloud-native services	A.5.23, A.8.8
Identity and access management	SSO, MFA, directory services, privilege escalation, orphaned accounts	A.8.5, A.8.2, A.5.16
Development and CI/CD pipelines	Source code exposure, deployment pipeline security, secrets in CI/CD	A.8.25, A.8.29, A.8.28
Third-party integrations	API keys, vendor access paths, supply chain component security	A.5.21, A.5.23
Endpoints and workstations	Endpoint protection, encryption validation, lateral movement from workstation	A.8.1, A.8.7, A.8.24
Logging and monitoring systems	Detection capability, log integrity, SIEM alert validation	A.8.15, A.8.16

What ISO 27001 Does Not Explicitly Require

- Specific penetration testing methodology (PTES, OWASP, NIST SP 800-115 are all acceptable - document your chosen methodology in the SoA/procedures).
- Mandatory use of an accredited or certified testing firm (unlike FedRAMP's 3PAO requirement).
- Physical penetration testing (relevant only if physical controls are in the ISMS scope).
- Social engineering campaigns (relevant if A.6.3 awareness training is in scope and social engineering risk is identified).
- Formal red team exercises (recommended for high-maturity organizations but not required for certification).
- Fixed testing cadence (annual is the industry standard and auditor expectation, but the standard says 'periodic').

08 What Certification Auditors Expect

EVIDENCE REQUIREMENTS FOR STAGE 2 AND SURVEILLANCE AUDITS

TYPICALLY EXPECTED	COMMONLY RECOMMENDED
- Annual penetration test - external and internal networks. - Web application / API pentest. - Cloud configuration review (AWS / Azure / GCP). - Vulnerability scanning program with documented cadence. - Statement of Applicability referencing A.8.8 and A.8.29. - Remediation evidence - tracked and closed before audit. - Retest confirmation on critical and high findings. - Pentest methodology documentation (in procedures or SoA).	- Security testing integrated into CI/CD pipeline (A.8.29). - Threat intelligence program feeding pentest scope (A.5.7). - Network segmentation validation testing (A.8.22). - Detection and response validation (SIEM alert testing - A.8.16). - Supply chain / third-party component security assessment (A.5.21). - Social engineering / phishing simulation (A.6.3). - Physical security assessment where physical assets are in scope.

What a Compliant ISO 27001 Pentest Report Should Include

- Scope definition referencing the ISMS boundary and specific systems tested.
- Methodology documentation - referenced standard (NIST SP 800-115, PTES, OWASP) with rationale.
- Findings mapped to specific ISO 27001:2022 Annex A controls (use 2022 numbering - not 2013).
- Severity ratings with CVSS scores and business impact in information security terms.
- Proof of exploitation - screenshots, request/response captures, attack chains.
- Risk treatment recommendations aligned to Annex A controls and ISO 27002 guidance.
- Retest confirmation - evidence that critical and high findings were remediated.
- Tester independence statement and relevant credentials (OSCP, CREST, CEH, or equivalent).
- Risk accepted / compensating controls documented for findings not remediated before audit.

09 Surveillance and Recertification Audits

MAINTAINING ISO 27001 CERTIFICATION OVER TIME

ISO 27001 certification is maintained through a three-year cycle: initial certification (Stage 1 + Stage 2), followed by two annual surveillance audits, and then a full recertification audit in year three. Penetration testing evidence is expected at every stage.

Audit Type	Timing	Pentest Evidence Expected
Stage 1 - Documentation Review	Initial certification	Pentest policy and procedures documented. Methodology selected and recorded in ISMS documentation.

Stage 2 - Implementation Audit	Initial certification (typically 3-6 months after Stage 1)	Recent pentest report (within 12 months) covering ISMS scope. Remediation evidence. A.8.8 and A.8.29 implementation demonstrated.
Surveillance Audit 1	12 months after certification	Updated pentest or new annual pentest. Evidence that previous findings are remediated. Vulnerability scanning logs.
Surveillance Audit 2	24 months after certification	Annual pentest covering any scope changes. Updated SoA if new systems added. Continued remediation evidence.
Recertification Audit	36 months after certification	Full ISMS re-evaluation. All pentest evidence for the three-year period. Trend analysis - are the same finding types recurring? Demonstrates continual improvement (Clause 10).

CONTINUAL IMPROVEMENT: CLAUSE 10

ISO 27001's Clause 10 (Improvement) requires that nonconformities are corrected and the root cause addressed to prevent recurrence. This applies directly to pentest findings. If the same vulnerability type (e.g., SQL injection, weak authentication) appears in consecutive annual pentests, auditors will question whether the SDLC and control improvements are working. Recurring findings without systemic remediation are a Clause 10 nonconformity - not just a technical finding. Use pentest trends over multiple years as evidence of continual ISMS improvement.

10

Resources

ISO 27001 AND PENTESTING REFERENCES

ISO/IEC 27001:2022 - Official Standard iso.org/standard/27001

The primary source. Purchase required. Defines all mandatory ISMS requirements including Clauses 4-10 and Annex A. Essential before any ISMS implementation or audit preparation.

ISO/IEC 27002:2022 - Controls Guidance iso.org/standard/75652

Implementation guidance for every Annex A control. Auditors use ISO 27002 to assess the depth of control implementation. Explicitly references penetration testing in A.8.8 and A.8.16 guidance.

Software Secured: NIST SP 800-115 and Pentesting softwaresecured.com

Explains how NIST SP 800-115 (the technical testing standard) relates to ISO 27001 and other compliance frameworks. Useful for scoping and methodology documentation.

NIST SP 800-115: Technical Guide to Information Security Testing csrc.nist.gov

The most widely referenced penetration testing methodology standard. Acceptable for ISO 27001 A.8.8 and A.8.29 methodology documentation. Free and authoritative.

OWASP Testing Guide v4.2 owasp.org

Industry-standard methodology for web application and API security testing. Directly applicable to A.8.26 (Application Security Requirements) and A.8.29 (Security Testing in Development).

CIS Controls v8 - Mapping to ISO 27001 cisecurity.org

CIS Controls map well to ISO 27001 Annex A. Useful for prioritizing control implementation and demonstrating defense-in-depth alongside ISO 27001 certification.

MITRE ATT&CK; Framework attack.mitre.org

Adversarial tactics and techniques framework. Useful for mapping pentest findings to real-world threat actor behavior - strengthens A.5.7 (Threat Intelligence) evidence and adds context to audit reports.

ISO 27001 Transition Guide: 2013 to 2022 iso.org

Official ISO guidance on transitioning from ISO 27001:2013 to 2022. Essential for understanding control number mapping (e.g., A.12.6.1 to A.8.8) when updating pentest report templates.

CREST: Penetration Testing Guidance crest-approved.org

CREST is a professional body for penetration testing. CREST-certified testers are widely recognized by ISO 27001 certification bodies as qualified independent assessors for A.8.8.