Regulatory intelligence report · Spain · Legal position as at 27 September 2026

Penetration Testing for SOC 2, ISO 27001, ENS and NIS2 in Spain (2026)

What each framework actually requires, what auditors expect in practice, and how one testing programme can evidence all four.

SOC 2 | ISO/IEC 27001 | ENS | NIS2

VERSION
1.0 · 27 September 2026

PUBLISHED BY
hacketico.es, a brand of Cyberscore B.V. (cyberscore.nl) · KVK 97451436

NEXT REVIEW
March 2027, or earlier if the Spanish NIS2 transposition law is published in the BOE

About this report

Purpose

This report sets out, as at 27 September 2026, what SOC 2, ISO/IEC 27001:2022, the *Esquema Nacional de Seguridad* (ENS, National Security Framework) and NIS2 require or expect of organisations in Spain in relation to penetration testing, and how to run a single testing programme whose evidence satisfies all four. It distinguishes throughout between what a legal text mandates, what a scheme makes auditable, what auditors expect in practice and what is simply good practice.

Audience

CISOs, security and GRC leads, DPOs and CTOs of organisations operating in Spain (SaaS and cloud providers, managed service providers, fintech, public-sector suppliers and multinationals with Spanish entities) and the penetration-testing providers who serve them. It assumes technical literacy and no legal background.

LEGAL NOTE · DISCLAIMER

This report is general information for security and compliance practitioners. It is not legal advice and does not create an adviser–client relationship. Regulatory status is stated as at 27 September 2026 and will change, in particular when Spain's NIS2 transposition law is published in the *Boletín Oficial del Estado* (BOE, Official State Gazette). Confirm the position with qualified counsel before relying on it.

Conventions

- Every legal or standards claim names its instrument and the article, control, criterion or measure identifier.
- Each requirement carries one of four badges (right). "Must" is reserved for badge A and badge B; "expect" signals badge C.
- Spanish official names appear in italics with an English gloss on first use. ENS measure identifiers are reproduced exactly as in Annex II of *Real Decreto 311/2022*.
- "Legal position as at 27 September 2026" appears in the running header of every page that describes regulatory status.
- Figures and tables are numbered by section. Three callout types recur: **Legal note**, **Auditor lens** and **Spain specific**.
- Sources are listed in Appendix 13.2. Items that could not be verified against the fact base as at the report date are flagged in Appendix 13.4; the change log is Appendix 13.5.

DOCUMENT CONTROL

Version
1.0

Date
27 September 2026

Legal position
as at 27 September 2026

Next review
March 2027, or earlier if the NIS2 transposition law is published in the BOE

Language
English (UK spelling)

Change log
Appendix 13.5, page 32

Publisher
hacketico.es, a brand of Cyberscore B.V. (cyberscore.nl), KVK-nummer 97451436

REQUIREMENT BADGES

`A · MANDATED`
The legal text itself requires the test.

`B · REQUIRED BY SCHEME`
The standard, certification scheme or the organisation's own declared controls make it auditable.

`C · AUDITOR EXPECTATION`
Not written, but auditors and regulators expect evidence in practice.

`D · RECOMMENDED`
Good practice.

FRAMEWORK COLOURS

SOC 2 · ISO/IEC 27001 · ENS · NIS2

Used identically on every page. Vermilion is reserved for badge A.

Contents

About this report · disclaimer · conventions 2

1 Executive summary 4

2 Why 2026 is different in Spain 5

Figure 2.1 · Dated timeline 2022 → 2027 6

2.5 · Adjacent regimes: GDPR, DORA, CRA, PCI DSS 7

3 Pentesting fundamentals for compliance 8

4 SOC 2: criteria, evidence, control language 10

5 ISO/IEC 27001:2022: controls, SoA, audit links 12

6 ENS: categories, measures, certification cycle 14

7 NIS2 in Spain: status, what binds now, what changes 17

8 One programme, four frameworks 20

9 Legal and contractual basis in Spain 22

10 Procuring a provider in Spain 24

11 Reporting: audit-ready reports, SLAs, attestation 26

12 Checklists and 90-day plan 28

13 Appendix 30

13.1 · Glossary (English / Spanish) 30

13.2 · References 31

13.3 · Watch list 13.4 · Items to verify 13.5 · Change log 32

FIGURES AND TABLES

Table 1.1 Framework × badge matrix · 4

Figure 2.1 Dated timeline 2022 → 2027 · 6

Table 3.1 Test types and compliance drivers · 8

Table 3.2 Scan, penetration test, red team · 9

Table 4.1 SOC 2 criterion mapping · 10

Table 5.1 ISO/IEC 27001 control mapping · 12

Figure 6.1 ENS category ladder · 14

Table 6.1 ENS measures by category · 15

Figure 6.2 ENS certification cycle · 16

Table 6.2 CCN-STIC guides for testing · 16

Table 7.1 IR (EU) 2024/2690 testing points · 18

Figure 8.1 Unified annual testing calendar · 20

Figure 8.2 Test once, evidence four times · 20

Table 8.1 Frequency matrix · 21

Table 8.2 Cross-mapping: artefact ↔ control ID · 21

Table 10.1 RFP evaluation sheet · 25

Figure 11.1 Anatomy of an audit-ready report · 26

Table 11.1 Remediation SLAs by severity · 26

Figure 12.1 90-day plan · 29

HOW TO USE

Read section 1 for the position, section 8 for the programme, and the framework section that matches your next audit. Sections 9 to 12 are operational and can be handed to procurement and delivery teams as they stand.

Reading paths

CISO, management body

Pages 4 · 5–7 · 17–19 · 28

Position, exposure and accountability: Table 1.1, the four clocks of 2026, what changes on BOE publication, the NIS2 checklist. About one hour.

GRC lead preparing an audit

Pages 10–19 · 20–21 · 26–29

The framework section for the audit in hand, then the unified calendar, cross-mapping table, report anatomy and readiness checklist.

DPO, legal counsel

Pages 7 · 22–23 · 32

GDPR Art. 32(1)(d) and the LOPDGDD, the *Código Penal* authorisation basis, processor terms, retention, and the items flagged for verification.

Penetration-testing provider

Pages 8–9 · 22–27

Vocabulary auditors accept, the legal basis of the engagement, the RFP requirements clients will send, and the report and letter they expect back.

SECTION 1

Executive summary

None of the four frameworks uses the same verb for penetration testing. One mandates it, one makes it auditable the moment you declare it, and two expect it without naming it. Table 1.1 states the position; the rest of this report shows how to satisfy all four with a single programme.

FRAMEWORK	INSTRUMENT AND PROVISION	BADGE	EXPECTED SCOPE	EXPECTED FREQUENCY · WHO CHECKS
SOC 2	AICPA TSP Section 100, 2017 Trust Services Criteria with Revised Points of Focus (2022): CC4.1, CC7.1, CC7.2–CC7.4, CC6.1, CC6.6, CC6.7, CC8.1, CC9.2	C → B once the system description names penetration testing	Components inside the described system boundary: external and internal network, web application and APIs, cloud configuration	At least one test per review period with remediation and retest evidence (Type II periods commonly 6–12 months). Checked by a licensed CPA firm.
ISO/IEC 27001	ISO/IEC 27001:2022 (Amd 1:2024). Annex A 8.8, 8.29, 8.25, 8.34, 5.35; clauses 6.1.3, 9.1, 9.2, 9.3, 10	C → B once the Statement of Applicability names penetration testing	Assets within the ISMS scope; development and acceptance testing under Annex A 8.29	Risk-based; auditors expect an annual cycle aligned to surveillance audits and major releases. Checked by an ENAC-accredited certification body.
ENS	*Real Decreto 311/2022*, Annex II: `[op.mon.3.r6.3]` (ALTA), `[op.mon.3.r2]` (MEDIA, ALTA), `[mp.s.2]`, `[op.nub.1.2]` (all categories), `[mp.sw.2]`, `[op.exp.4]`; Art. 31 audits	A penetration tests at ALTA; web-application audits and cloud requirements at all categories	Systems within the declaration of applicability; web applications before production; third-party cloud services	No numeric frequency in the text: set by the audit procedure and risk analysis. Art. 31 audit at least every two years and after substantial change. Certification body (MEDIA, ALTA); self-assessment (BÁSICA).
NIS2	Directive (EU) 2022/2555 Art. 21(2)(e), Art. 21(2)(f), Art. 20; Commission Implementing Regulation (EU) 2024/2690, Annex points 6.5, 6.10, 7	B Art. 21(2)(f) A IR 2024/2690 point 6.5, for the entities it covers	Network and information systems used to provide the essential or important service	As set in the entity's own security-testing policy, reviewed at planned intervals (point 6.5). National authorities: Spanish designation pending a transposition law that is not in force as at 27 September 2026.

Table 1.1 Framework × badge matrix, with expected scope and frequency at a glance.

01

Only two texts mandate a test in Spain today. ENS Annex II does so at category ALTA (`[op.mon.3.r6.3]`) and for web applications at every category (`[mp.s.2]`); Implementing Regulation (EU) 2024/2690 point 6.5 does so for the digital-infrastructure and digital-provider entities it lists.

02

SOC 2 and ISO/IEC 27001 never legally require a penetration test. Neither names one. Both become auditable (badge B) the moment your own system description or Statement of Applicability names one, and both are examined against what you wrote.

03

Spain's NIS2 law is not in force. As at 27 September 2026 the transposition bill has not been published in the BOE. The directive's Arts 20, 21 and 23 already fix the substance, and the Implementing Regulation applies directly; the penalty regime becomes enforceable in Spain only once the national law is published.

A · MANDATED — The legal text itself requires the test

B · REQUIRED BY SCHEME — Standard, scheme or own declared controls make it auditable

C · AUDITOR EXPECTATION — Not written; evidence expected in practice

D · RECOMMENDED — Good practice

SECTION 2

Why 2026 is different in Spain

Four regulatory clocks are running at different speeds. Together they make 2026 the year in which a documented, repeatable testing programme stops being good practice and becomes the cheapest way to answer every auditor at once.

2.1 NIS2: late, but not dormant

Directive (EU) 2022/2555 (NIS2) had to be transposed by 17 October 2024. Spain missed the deadline. The transposition vehicle, the *Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad* (draft Cybersecurity Coordination and Governance Act), was approved by the Council of Ministers at first reading on 14 January 2025. As at 27 September 2026 it has not been enacted, has not been published in the BOE and is not in force. Infringement procedure INFR(2024)0270 continues (reasoned opinion 7 May 2025; 2026 stage to be verified, Appendix 13.4).

Two things already bind. Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 applies directly to the digital-infrastructure and digital-service entities it lists, without any Spanish act, and its Annex point 6.5 requires a security-testing policy. And the directive's Arts 20, 21 and 23 fix the substance that the Spanish law must carry; the draft mirrors them.

SPAIN SPECIFIC

Until the new law is in force, *Real Decreto-ley 12/2018* and *Real Decreto 43/2021* (Spain's NIS1 transposition) remain the applicable NIS framework. Reference CSIRTs: CCN-CERT (public sector), INCIBE-CERT (private sector and citizens) and ESPDEF-CERT (defence).

The draft law would create a *Centro Nacional de Ciberseguridad* (CNC, National Cybersecurity Centre) as coordinating authority and split supervision between the Ministry of the Interior, Defence through the *Centro Criptológico Nacional* (CCN, National Cryptologic Centre) and Digital Transformation through INCIBE.

LEGAL NOTE

"Not in force" means the draft has no legal effect: no Spanish authority can yet impose NIS2 penalties and no Spanish transitional deadline exists. There is no "October 2026 NIS2 deadline" in Spain. What does exist is directly applicable EU law (Implementing Regulation (EU) 2024/2690) and a directive whose text the national law must transpose. This report does not predict an entry-into-force date.

2.2 ENS: a mature scheme in mid-cycle

Real Decreto 311/2022, de 3 de mayo (BOE 4 May 2022) has been in force for more than four years. Its consolidated text was last amended with effect from 7 November 2024 by *Real Decreto 1125/2024*, which left the Annex II measures untouched. Art. 31 requires a regular audit at least every two years, so systems audited in 2024 fall due again in 2026. Private providers whose systems support public-sector services are within scope under Art. 2, and *Ley 9/2017, de Contratos del Sector Público* (LCSP, Public Sector Contracts Act) contracts flow ENS obligations down to them. ENS is the only framework in this report whose text names penetration tests directly (`[op.mon.3.r6.3]`).

2.3 DORA testing is live

Regulation (EU) 2022/2554 (DORA) has applied since 17 January 2025. Arts 24–27 govern testing; Art. 26 requires threat-led penetration testing (TLPT) at least every three years for designated financial entities, under Commission Delegated Regulation (EU) 2025/1190 (OJ 18 June 2025, applicable 8 July 2025), aligned with TIBER-EU as updated in February 2025. Financial entities' ICT providers inherit these testing expectations through contract.

AUDITOR LENS

Auditors do not wait for the BOE. SOC 2 and ISO/IEC 27001 auditors already ask NIS2-scope clients how they assess the effectiveness of their measures (Art. 21(2)(f)); the answer they recognise is a dated, scoped penetration-test report with remediation evidence.

2.4 CRA reporting has started

Under Regulation (EU) 2024/2847 (Cyber Resilience Act), manufacturers' reporting obligations have applied since 11 September 2026; the main obligations follow on 11 December 2027. Manufacturers of products with digital elements now need a vulnerability-handling process fed by real testing, and their reports become evidence.

The dated record, 2022 → 2027

2022

- 4 May 2022 *Real Decreto 311/2022* **published in the BOE.** New ENS: 73 Annex II measures, three categories, audit at least every two years (Art. 31).
- 2022 **Directive (EU) 2022/2555 (NIS2) and Regulation (EU) 2022/2554 (DORA) adopted.**

2023

- ○ No dated milestone within this report's fact base.

2024

- 17 Oct 2024 **NIS2 transposition deadline passes without a Spanish law.** Commission Implementing Regulation (EU) 2024/2690 adopted the same day; it applies directly to the digital entities it lists.
- 7 Nov 2024 *Real Decreto 1125/2024* **amendments to the ENS take effect.** Annex II measures unchanged.

2025

- 14 Jan 2025 **Draft** *Ley de Coordinación y Gobernanza de la Ciberseguridad* **approved at first reading** by the Council of Ministers.
- 17 Jan 2025 **DORA applies.** Arts 24–27 testing; Art. 26 TLPT at least every three years for designated entities. TIBER-EU updated in February 2025.
- 7 May 2025 **Commission reasoned opinion** in infringement procedure INFR(2024)0270.
- 18 Jun 2025 **Delegated Regulation (EU) 2025/1190 (TLPT technical standards) published in the OJ;** applicable 8 July 2025.
- 31 Oct 2025 **ISO/IEC 27001 transition closes.** Certificates to the 2013 edition are no longer valid.

2026

- 2026 **INFR(2024)0270 escalation continues.** Exact stage to be verified before publication.
- 11 Sep 2026 **Cyber Resilience Act reporting obligations for manufacturers apply** (Regulation (EU) 2024/2847).

> 27 Sep 2026 **This report.** Spanish NIS2 transposition law not enacted, not in the BOE, not in force.

2027

- ○ Mar 2027 **Next review of this report,** or earlier if the Spanish NIS2 law is published in the BOE.
- 11 Dec 2027 **Cyber Resilience Act main obligations apply.**

Figure 2.1 Dated timeline 2022 → 2027. Every date is taken from the fact base verified as at 27 September 2026. Dots: ● ENS ● NIS2 ● ISO/IEC 27001 ● other EU law. SOC 2 has no dated event: no new Trust Services Criteria were issued for 2025 or 2026.

READING THE TIMELINE

Fixed. ENS measures, ISO/IEC 27001:2022, the 2017 SOC 2 criteria, DORA and the Implementing Regulation are settled texts. Programmes built on them will not need rework.

Pending. The Spanish NIS2 law. Its content is largely knowable from the directive and the draft; its dates are not. Nothing in this report assumes a date.

Next. CRA main obligations on 11 December 2027 will pull product security testing into conformity evidence for manufacturers.

AUDITOR LENS

Auditors read status statements for their date. Any internal paper on NIS2 readiness should carry its own "as at" date, as this report does, and should be re-issued when the BOE publication changes the position.

WHAT EACH MILESTONE MEANS FOR THE TESTING PROGRAMME

MILESTONE	CONSEQUENCE FOR SCOPE, METHOD OR EVIDENCE	BADGE
4 May 2022 · ENS in force	Category, Annex II measures and the Art. 31 two-year cycle set test scope and rhythm for public-sector systems and their private suppliers	A
17 Oct 2024 · IR (EU) 2024/2690	Listed digital entities need a written security-testing policy and a documented methodology now, without waiting for Spanish law	A
17 Jan 2025 · DORA applies	Financial entities run a testing programme; designated ones add TLPT every three years; their ICT providers inherit the requirements by contract	A
31 Oct 2025 · ISO transition closed	Statements of Applicability must be written against the 2022 control set (8.8, 8.29, 8.34); 2013 wording is no longer certifiable	C
11 Sep 2026 · CRA reporting	Manufacturers report actively exploited vulnerabilities; product test findings feed that process and the 2027 conformity file	A
27 Sep 2026 · Spanish NIS2 law pending	Build to Arts 20, 21 and 23 now; penalties unenforceable in Spain until publication in the BOE; no transitional date exists	B

A · MANDATED — The legal text itself requires the test

B · REQUIRED BY SCHEME — Standard, scheme or own declared controls make it auditable

C · AUDITOR EXPECTATION — Not written; evidence expected in practice

D · RECOMMENDED — Good practice

2.5 Adjacent regimes that shape the programme

Four further instruments touch penetration testing in Spain. None replaces the four frameworks in this report, but each adds a scope, a frequency or a contractual pull that the programme in section 8 must absorb.

GDPR and LOPDGDD

Regulation (EU) 2016/679 Art. 32(1)(d) · *Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales* (LOPDGDD) · supervisory authority: *Agencia Española de Protección de Datos* (AEPD, Spanish Data Protection Agency)

A regular testing of measures C penetration testing as the form

Art. 32(1)(d) requires controllers and processors to implement, as appropriate to the risk, "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures". It does not name penetration testing, but an independent test is the most widely recognised evidence that the process exists and works for systems holding personal data.

Effect on the programme. The tester becomes a processor (Art. 28) whenever the systems in scope hold personal data; section 9 sets out the contract terms and the breach-notification path if a test uncovers an actual compromise.

DORA

Regulation (EU) 2022/2554, applicable since 17 January 2025 · Arts 24–27 · Commission Delegated Regulation (EU) 2025/1190 (OJ 18 June 2025, applicable 8 July 2025) · TIBER-EU (updated February 2025)

A testing programme, Arts 24–25 A TLPT every three years, Art. 26, designated entities

Financial entities in scope must run a digital operational resilience testing programme (Art. 24) whose test types include penetration testing (Art. 25). Designated entities must perform threat-led penetration testing at least every three years (Art. 26) using testers meeting Art. 27, under the technical standards in Delegated Regulation (EU) 2025/1190, aligned with TIBER-EU. In Spain the TIBER-ES programme is led by Banco de España; current TLPT-authority designations should be verified before naming them (Appendix 13.4).

Effect on the programme. ICT third-party providers to financial entities inherit testing evidence requests through contract and, where they support critical functions, may fall inside a TLPT scope.

Cyber Resilience Act

Regulation (EU) 2024/2847 · manufacturers' reporting obligations apply from 11 September 2026 · main obligations from 11 December 2027

D product testing today A vulnerability-handling requirements from 11 December 2027

Since 11 September 2026 manufacturers of products with digital elements must report actively exploited vulnerabilities and severe incidents (Art. 14). From 11 December 2027 the essential requirements apply, including the Annex I Part II vulnerability-handling requirements, which call for effective and regular security tests and reviews of the product (exact point numbering: verify, Appendix 13.4).

Effect on the programme. Product manufacturers should fold product penetration tests into technical documentation now and align disclosure with NIS2 Art. 21(2)(e) and Implementing Regulation (EU) 2024/2690 point 6.10.

PCI DSS v4.0.1 (comparator only)

Payment Card Industry Data Security Standard v4.0.1, Requirement 11.4 · contractual scheme of the card brands, not law

B explicit penetration-testing mandate for entities in cardholder-data scope

Requirement 11.4 is what an explicit mandate looks like: a defined methodology, external and internal penetration testing at least once every 12 months and after significant changes, remediation of exploitable vulnerabilities and retesting. None of SOC 2, ISO/IEC 27001 or NIS2 is written this way; ENS comes closest at category ALTA (`[op.mon.3.r6.3]`).

Effect on the programme. If cardholder data is in scope, the 11.4 test is the natural anchor of the annual calendar in section 8; the other frameworks accept its report as evidence when the scope covers their boundary.

A · MANDATED — The legal text itself requires the test

B · REQUIRED BY SCHEME — Standard, scheme or own declared controls make it auditable

C · AUDITOR EXPECTATION — Not written; evidence expected in practice

D · RECOMMENDED — Good practice

SECTION 3

Pentesting fundamentals for compliance

Auditors accept a test as evidence only when its type, depth and method match the control it is meant to prove. This section fixes the vocabulary the rest of the report uses.

TEST TYPE	WHAT IT EXAMINES	TYPICAL COMPLIANCE DRIVER	PRACTICAL NOTE
External network	Internet-facing hosts, perimeter services, VPN and remote-access gateways, exposed management interfaces	SOC 2 CC6.6 · ISO 8.8 · ENS `[op.mon.3.r6.3]` · NIS2 Art. 21(2)(f)	The test auditors ask for first. Scope by IP range and domain list.
Internal network	Lateral movement, directory and identity services, privilege escalation, segmentation between zones	SOC 2 CC6.1 · ISO 8.8 · ENS `[op.mon.3.r6.3]`	Needs on-site or VPN access; agree segments and crown-jewel targets in advance.
Web application	Authentication, session management, access control, injection, business logic (OWASP WSTG)	ENS `[mp.s.2]` · ISO 8.29 · SOC 2 CC6.1, CC8.1	ENS requires audits during development and before production.
API	Authentication and authorisation per endpoint and object, input validation, rate limiting, schema conformance	ISO 8.26, 8.29 · SOC 2 CC6.1	Provide the specification (OpenAPI) and one test account per role.
Mobile	Client-side storage, transport security, platform protections, backend calls	ISO 8.26 · SOC 2 CC6.7	Test each published platform; the backend is usually covered by the API test.
Cloud configuration	Identity and access, storage exposure, network policy, logging, key management, tenant isolation	SOC 2 CC6.1, CC7.1 · ISO 8.8 · ENS `[op.nub.1.2]`	Read-only configuration review plus validation; respect the provider's testing policy (section 9).
Wireless	Enterprise Wi-Fi authentication, rogue access points, guest-network segmentation	ISO 8.8 · ENS `[op.mon.3]`	Physical presence required; often bundled with internal testing.
Social engineering	Staff response to phishing, vishing and pretexting	SOC 2 CC4.1 (evaluation) · NIS2 Art. 20 (training)	HR, legal and works-council sign-off; no capture of personal data.
Physical	Site access control, tailgating, unattended devices, document handling	ISO Annex A 7.1–7.14 (physical controls)	Testers carry the written authorisation; agree stop rules.
Red team / TLPT	Objective-based, intelligence-led adversary simulation across people, process and technology	DORA Art. 26 (designated entities) · NIS2 Art. 21(2)(f) as an effectiveness assessment	Supplements coverage testing; never replaces it.

Table 3.1 Test types, what they examine and the provisions that most often drive them. ISO references are to ISO/IEC 27001:2022 Annex A.

3.1 Black, grey and white box

Black box

No prior knowledge or credentials; the tester works as an external attacker would. ENS `[mp.s.2]` R1 names continuous black-box audits of web applications as one option at BÁSICA and MEDIA. Coverage depends on what the tester can discover.

Grey box

Credentials for defined roles plus architecture documentation. The most efficient approach for applications, APIs and cloud, and the usual default for SOC 2 and ISO/IEC 27001 evidence because it maximises verified coverage per testing day.

White box

Full access including source code and configuration. ENS `[mp.s.2]` R2 requires white-box audits with defined methodologies and automated vulnerability tools; category ALTA requires R2 and R3. `[mp.sw.2]` R2 adds an optional source-code audit.

3.2 Vulnerability scan, penetration test, red team

	VULNERABILITY SCAN	PENETRATION TEST	RED TEAM / TLPT
Purpose	Enumerate known vulnerabilities and misconfigurations at breadth	Exploit and chain weaknesses to demonstrate real impact within an agreed scope	Test detection and response against defined objectives, as an adversary would
Method	Automated tooling; version and signature checks; authenticated where possible	Manual testing led by a documented methodology, supported by tools	Intelligence-led scenarios (TIBER-EU), covert, with a control team and an unaware blue team
Effort	Minutes to hours, plus analyst triage	Days to weeks per scope	Weeks to months
Output	List of candidate findings with CVSS scores; false positives expected	Report of verified findings with evidence, business impact, remediation and retest	Attack-path narrative, detection gaps, response timeline, purple-team replay
Cadence	Continuous or monthly	Annual and after significant change; ENS: as the audit procedure sets	DORA Art. 26: at least every three years for designated entities; otherwise risk-based
Named in	SOC 2 CC7.1 (vulnerability scans) · ENS `[op.mon.3.r2]`, `[op.mon.3.r6.2]` · IR (EU) 2024/2690 point 6.10	SOC 2 CC4.1 point of focus · ISO/IEC 27002:2022 guidance to 8.8 · ENS `[op.mon.3.r6.3]` · IR (EU) 2024/2690 point 6.5	DORA Arts 26–27 · Delegated Regulation (EU) 2025/1190 · TIBER-EU, TIBER-ES

Table 3.2 Three activities that auditors routinely see conflated. A scan report relabelled as a penetration test is the most common evidence rejection.

3.3 Methodology standards

OWASP Web Security Testing Guide (WSTG). Test cases for web applications; cite WSTG identifiers against each finding.

OWASP Application Security Verification Standard (ASVS) 5.0. Verification requirements at three levels; use as acceptance criteria under ISO 8.29 and ENS `[mp.sw.2]`.

PTES. Penetration Testing Execution Standard: a seven-phase engagement process from pre-engagement to reporting.

NIST SP 800-115. Technical Guide to Information Security Testing and Assessment: planning, execution and post-execution; widely cited by SOC 2 auditors.

OSSTMM. Open Source Security Testing Methodology Manual; operational security metrics across channels.

MITRE ATT&CK. Adversary tactics and techniques; map red-team activity and detection coverage to it.

CCN-STIC 802 and 808. The ENS audit and compliance-verification method the certification auditor will apply to your evidence.

3.4 Severity scoring

CVSS v4.0. Base metrics describe the vulnerability; Threat and Environmental metrics adjust for exploit maturity and your own context; Supplemental metrics add information without changing the score. Report the full vector string, not only the number.

EPSS. The probability that a published CVE will be exploited in the wild within the next 30 days. Use it to order remediation among findings of equal CVSS severity.

Business context. Asset criticality, data classification, exposure, compensating controls and regulatory scope (ENS category, DORA critical function). The resulting rating, not the raw CVSS score, drives the remediation SLAs in section 11.

AUDITOR LENS

The severity model must be written down and applied consistently across periods. Re-rating a finding downwards is legitimate only with a recorded justification signed by the risk owner; silent re-rating is read as evidence manipulation.

SECTION 4 SOC 2

SOC 2: an attestation, not a mandate

The Trust Services Criteria never require a penetration test. They require evaluations, vulnerability detection, response and change control, and their points of focus name penetration testing as one way to show them.

SOC 2 is an attestation report issued by a licensed CPA firm under AICPA attestation standards. The auditor examines management's description of the system and the design (Type I, at a point in time) or the design and operating effectiveness (Type II, over a period commonly of 6 to 12 months) of controls against AICPA TSP Section 100, the 2017 Trust Services Criteria with Revised Points of Focus (2022). No new criteria have been issued for 2025 or 2026. Security, expressed as Common Criteria CC1 to CC9, is the only mandatory category.

LEGAL NOTE

SOC 2 is not law and is not a certification. Its force is contractual: customers require the report and read the exceptions. Nothing in the criteria "legally requires" a penetration test, and this report never says so.

Because the criteria describe outcomes rather than techniques, penetration testing enters a SOC 2 examination through the organisation's own words. Once the system description or a listed control states that an annual test is performed, that statement is the control the auditor tests, literally and against evidence; the badge moves from C to B at that moment.

CRITERION	WHAT THE CRITERION ASKS	HOW PENETRATION TESTING EVIDENCES IT	BADGE
CC4.1	Ongoing and/or separate evaluations of whether internal-control components are present and functioning; the points of focus name penetration testing as an evaluation type	An independent test is a "separate evaluation": scope approved, results reviewed and deficiencies communicated to those responsible	C
CC7.1	Detection and monitoring procedures to identify configuration changes and newly introduced vulnerabilities; vulnerability scans	Scan cadence plus a periodic test that validates scan coverage and finds what scanners miss	C
CC7.2	Monitoring of system components for anomalies indicative of malicious acts	Were the testers' activities logged and alerted? Report the detection outcome as a finding in its own right	C
CC7.3	Evaluation of security events to determine whether they could or have resulted in a failure to meet objectives	Triage of each finding: severity, affected objective, decision recorded	C
CC7.4	Response to identified security incidents through a defined incident-response programme	Remediation workflow: ticket, owner, due date, fix, retest; escalation if a test finds an actual compromise	C
CC6.1	Logical access security software, infrastructure and architectures over protected information assets	Authentication, authorisation and privilege-escalation findings on applications, APIs and cloud identity	C
CC6.6	Security measures against threats from sources outside the system boundaries	External network and perimeter test; exposed services reconciled to the asset inventory	C
CC6.7	Restriction of the transmission, movement and removal of information; protection in transit	TLS configuration, certificate handling and data-in-transit findings	C
CC8.1	Changes are authorised, designed, developed, configured, documented, tested, approved and implemented	Pre-release application testing tied to change records; "after significant changes" clause evidenced	C
CC9.2	Assessment and management of risks associated with vendors and business partners	Review of sub-service organisations' own test evidence or SOC 2 reports; carve-out or inclusive method stated	C

Table 4.1 SOC 2 criterion mapping. Every row is badge C by default and becomes badge B once the system description names penetration testing.

A · MANDATED — The legal text itself requires the test

B · REQUIRED BY SCHEME — Standard, scheme or own declared controls make it auditable

C · AUDITOR EXPECTATION — Not written; evidence expected in practice

D · RECOMMENDED — Good practice

4.2 Evidence auditors request

1. **Signed scope and rules of engagement**, dated within the review period, naming the components tested and those excluded.
2. **Final report**: methodology, dates, named testers, findings with severity, evidence and remediation advice.
3. **Independence and qualifications statement** for the testing team.
4. **Remediation tracker**: finding → ticket → owner → due date → closure evidence (CC7.4, CC8.1).
5. **Retest report or attestation letter** confirming closure of Critical and High findings (section 11).
6. **Management review record**: minutes or sign-off showing results were communicated to those responsible and decisions taken (CC4.1).
7. **Coverage reconciliation**: asset inventory matched to the tested scope; exclusions justified in writing.
8. **Sub-service organisations** (cloud, hosting): their SOC 2 report or bridge letter and your documented review of it (CC9.2).

4.3 Sample control language for the system description

`Example control · maps to CC4.1, CC7.1, CC7.4, CC8.1`

The Organisation engages an independent third party to perform a penetration test of the production environment supporting the Service at least annually and after significant changes to the network architecture or the application. The scope covers the external and internal network infrastructure, the web application and the APIs within the system boundary, and is approved in writing by the Head of Security before testing begins.

Findings rated Critical or High are remediated within the timeframes defined in the Vulnerability Management Policy and retested by the provider. Results, remediation status and residual risk are reported to the Security Steering Committee at its next meeting and tracked to closure in the risk register.

Tests of the control the auditor will perform: inspect the signed rules of engagement; inspect the report and confirm its date falls in the period; select a sample of High findings and trace them to tickets and closure; inspect the retest letter; inspect committee minutes.

AUDITOR LENS · TIMING

For a Type II period the auditor looks for a test performed inside the period and remediation evidenced inside it. A test completed shortly before the period start is often accepted where remediation and retest fall within the period, but only if the control text allows it.

For a Type I, the control must be designed and the test scheduled or completed by the report date.

AUDITOR LENS · WORDING

Write only what you will do. "At least annually" and "after significant changes" each generate an evidence request; an undefined "significant" becomes an exception when the auditor and you disagree about a release. Define it in the change-management policy and cite it.

TYPE I AND TYPE II

Type I reports on the design of controls at a point in time.

Type II reports on design and operating effectiveness over a period, commonly 6 to 12 months. Penetration-test evidence must show the control operated during that period.

SECTION 5 ISO/IEC 27001

ISO/IEC 27001:2022: the test your SoA describes

No Annex A control is called "penetration test". Ten controls and five clauses depend on one, and the Statement of Applicability is where you decide how auditable you make it.

ISO/IEC 27001:2022 (with Amd 1:2024) certifies that an information security management system exists, is risk-driven and operates as documented. In Spain, certificates are issued by ENAC-accredited bodies. The transition from the 2013 edition closed on 31 October 2025; certificates to the 2013 edition are no longer valid. The controls below ask for vulnerability management, security testing in development, monitoring and independent review, and the ISO/IEC 27002:2022 guidance to control 8.8 names penetration testing and vulnerability assessment as inputs. The auditor examines what the Statement of Applicability says you do: once it names penetration testing, the badge moves from C to B.

LEGAL NOTE

ISO/IEC 27001 is a voluntary standard. It binds only through contract, or where a law or scheme adopts it. It never legally requires a penetration test, and this report does not say it does.

CONTROL	TITLE (ANNEX A)	RELEVANCE TO PENETRATION TESTING	BADGE
8.8	Management of technical vulnerabilities	Obtain information about vulnerabilities, evaluate exposure, act. ISO/IEC 27002:2022 guidance names penetration testing and vulnerability assessment as inputs; the test report is the primary evidence.	C
8.29	Security testing in development and acceptance	Security testing processes defined and implemented in the development life cycle; a penetration test of a release before acceptance is the recognised form.	C
8.25	Secure development life cycle	Rules for secure development, including where security testing sits in the cycle and who signs it off.	C
8.26	Application security requirements	The requirements the test verifies: authentication, authorisation, cryptography, input validation, logging.	C
8.16	Monitoring activities	Whether tester activity was detected and escalated; feed the outcome back as a finding.	C
8.31	Separation of development, test and production environments	Run tests in pre-production where possible; production testing needs the additional planning in 8.34.	C
8.32	Change management	Test results as a gate for significant changes; the "after significant change" trigger lives here.	C
8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management. This is the control that governs how a test is authorised, timed and contained.	C
5.35	Independent review of information security	An independent penetration test is one input to the planned independent review of the approach to managing security.	C
5.36	Compliance with policies, rules and standards	Technical compliance review of systems against the organisation's own rules; the test verifies that the rules hold in practice.	C

Table 5.1 ISO/IEC 27001:2022 Annex A control mapping. Every row is badge C by default and becomes badge B once the Statement of Applicability names penetration testing as the implementing control.

A · MANDATED
The legal text itself requires the test

B · REQUIRED BY SCHEME
Standard, scheme or own declared controls make it auditable

C · AUDITOR EXPECTATION
Not written; evidence expected in practice

D · RECOMMENDED
Good practice

5.2 Management-system clauses that consume the test

CLAUSE	WHAT IT REQUIRES	WHERE PENETRATION TESTING FITS
6.1.3	Risk treatment: select controls, produce the Statement of Applicability with justifications	The justification for 8.8 and 8.29 names the risks the test treats; the frequency written there becomes auditable
9.1	Monitoring, measurement, analysis and evaluation	Metrics: findings by severity, mean time to remediate, retest closure rate, coverage of scope
9.2	Internal audit at planned intervals	Internal audit samples one test end to end: authorisation (8.34), report, tickets, retest, communication
9.3	Management review of the ISMS, including monitoring and audit results and nonconformities	Test results, open Critical and High findings and risk-acceptance decisions are a standing input
10	Improvement: nonconformity, corrective action, continual improvement	A finding that shows a control failed (not merely a missing patch) is raised as a nonconformity with root cause

5.3 Statement of Applicability wording

Example SoA entries

A 8.8 Management of technical vulnerabilities. Applicable. Justification: risk treatment (risks R-07 and R-12), contractual (customer security schedules) and legal (GDPR Art. 32(1)(d)). Implementation: authenticated vulnerability scanning of all in-scope assets at least monthly; independent penetration testing of internet-facing systems and the Platform application at least annually and before major releases, under procedure PRC-SEC-07; findings recorded in the vulnerability register and remediated within the timeframes of POL-VULN-01.

A 8.29 Security testing in development and acceptance. Applicable. Implementation: security acceptance criteria (OWASP ASVS 5.0 Level 2) verified before production; no release with open Critical or High findings without a documented risk acceptance by the Service Owner.

5.4 Internal audit and management review

Internal audit (9.2). Put the testing programme on the audit programme once a year and have the internal auditor sample one test end to end. It is the same chain the certification auditor follows, so a clean internal audit predicts a clean external one.

Management review (9.3). Present findings by severity and age, remediation against SLA and coverage against the ISMS scope, and record risk-acceptance decisions. Those records are what the auditor reads when a High finding is still open at the next visit.

AUDITOR LENS

Certification auditors verify that the SoA is implemented as written. A frequency you state and do not meet is a nonconformity even though the standard itself sets none. Keep SoA wording at the level you can evidence every year and put the detail in the procedure it cites.

SPAIN SPECIFIC

CCN-STIC 825 maps ISO/IEC 27001:2022 to the ENS. Organisations holding both can present one testing programme against 8.8 and 8.29 on one side and `[op.mon.3]` and `[mp.s.2]` on the other, provided the ISMS scope and the ENS category are reconciled in writing.

EDITION STATUS

ISO/IEC 27001:2022 with Amd 1:2024 is the only certifiable edition since 31 October 2025.

Amd 1:2024 adds climate-change considerations to clauses 4.1 and 4.2 and does not alter Annex A (wording to verify, Appendix 13.4).

SECTION 6 ENS

ENS: the framework that names the test

The ENS is the only framework in this report whose legal text requires penetration tests: at category ALTA through [op.mon.3.r6.3], and for every web application through [mp.s.2].

The ENS is established by *Real Decreto 311/2022, de 3 de mayo* (BOE 4 May 2022); its consolidated text was last amended with effect from 7 November 2024 by *Real Decreto 1125/2024*, which did not alter the Annex II measures. It applies to public-sector entities and to private-sector providers whose systems support public-sector services (Art. 2). Systems are categorised BÁSICA, MEDIA or ALTA by the impact of an incident, and Annex II sets 73 measures, many with reinforcements (*refuerzos*, R1, R2 …) that apply as the category rises or as the entity opts in.

Conformity is demonstrated by audit. Art. 31 requires a regular audit at least every two years and an extraordinary audit after substantial changes. Category BÁSICA may self-assess and issue a *declaración de conformidad* (declaration of conformity); MEDIA and ALTA require certification by a body accredited by ENAC (*Entidad Nacional de Acreditación*, National Accreditation Body), under the *Instrucción Técnica de Seguridad* (ITS, Security Technical Instruction) de Conformidad (*Resolución de 13 de octubre de 2016*) and the ITS de Auditoría (*Resolución de 27 de marzo de 2018*).

Penetration testing appears by name. Measure [op.mon.3] *Vigilancia* (monitoring), reinforcement R6 *Inspecciones de seguridad* (security inspections), requires, periodically or after incidents revealing new or underestimated vulnerabilities, configuration verification [op.mon.3.r6.1], vulnerability analysis [op.mon.3.r6.2] and penetration tests [op.mon.3.r6.3]. R6 is required at category ALTA. The ENS sets no numeric frequency: the rhythm flows from the audit procedure and the risk analysis, and in practice from the two-year audit cycle.

LEGAL NOTE

Badge A applies because Annex II is part of a royal decree: the text itself requires the test. A reinforcement marked required at a category is mandatory there; reinforcements the text calls optional are badge D, and this report keeps the two apart.

SPAIN SPECIFIC

The *Centro Criptológico Nacional* (CCN) publishes the CCN-STIC 800 series that auditors apply: 802 (audit), 808 (verification of compliance), 809 (declaration and certification of conformity), 823 (cloud services), 825 (ISO/IEC 27001:2022 to ENS mapping) and 817 (incident management). Cite the guide and version in the test plan.

BÁSICA

SELF-ASSESSMENT · *declaración de conformidad*

[mp.s.2] R1 or R2 web-application security audits

[op.nub.1.2] cloud services: ENS-conformant or CCN-STIC guide incl. pentesting audit

[mp.sw.2] security acceptance criteria before production

[op.exp.4] vulnerability tracking and patch prioritisation

MEDIA

CERTIFICATION · ENAC-ACCREDITED BODY

Everything at BÁSICA, plus:

[op.mon.3] R2 dynamic analysis of the exposure surface

[mp.sw.2] R1 tests in an isolated pre-production environment

[op.exp.4] R1 pre-production testing of updates

[mp.sw.1] R1–R4 secure development methodology

ALTA

CERTIFICATION · ENAC-ACCREDITED BODY

Everything at MEDIA, plus:

[op.mon.3] R6 security inspections: [op.mon.3.r6.1] configuration verification, [op.mon.3.r6.2] vulnerability analysis, [op.mon.3.r6.3] penetration tests

[mp.s.2] R2 and R3 web-application audits

[op.exp.4] R2 rollback capability

Figure 6.1 ENS category ladder: testing-related Annex II measures by category. Requirements cumulate upwards. Optional reinforcements ([mp.sw.2] R2 source-code audit, [op.exp.4] R4 continuous monitoring) are shown in Table 6.1.

6.2 Testing-related measures, category by category

MEASURE	WHAT ANNEX II REQUIRES	BÁSICA	MEDIA	ALTA	BADGE
`[op.mon.3]` R6 *Inspecciones de seguridad*	Periodically, or after incidents revealing new or underestimated vulnerabilities: configuration verification `[op.mon.3.r6.1]`, vulnerability analysis `[op.mon.3.r6.2]` and penetration tests `[op.mon.3.r6.3]`	—	—	**Required**	A at ALTA
`[op.mon.3]` R2 *Análisis dinámico*	Tooling that determines the exposure surface in terms of vulnerabilities and configuration weaknesses	—	**Required**	**Required**	A at MEDIA, ALTA
`[mp.s.2]` *Protección de servicios y aplicaciones web*	Security audits of web applications. R1: continuous black-box audits during development and before production, frequency set in the audit procedure. R2: white-box audits during development, defined methodologies plus automated vulnerability tools, findings fixed via `[op.exp.5]`. R3 adds to R2 at ALTA	**R1 or R2**	**R1 or R2**	**R2 + R3**	A all categories
`[op.nub.1.2]` *Protección de servicios en la nube*	Third-party cloud services must run on ENS-conformant systems or meet a CCN-STIC guide that includes requirements on, among others, "auditoría de pruebas de penetración (pentesting)"	**Required**	**Required**	**Required**	A all categories
`[mp.sw.2]` *Aceptación y puesta en servicio*	Security acceptance criteria verified before production. R1: tests in an isolated pre-production environment. R2: source-code audit (optional reinforcement)	**Base**	**Base + R1**	**Base + R1**	A base, R1 · D R2
`[op.exp.4]` *Mantenimiento y actualizaciones de seguridad*	Vulnerability tracking and patch prioritisation. R1: pre-production testing of updates. R2: rollback. R4: continuous threat and vulnerability monitoring (optional)	**Base**	**Base + R1**	**Base + R1 + R2**	A base, R1, R2 · D R4
`[mp.sw.1]` *Desarrollo de aplicaciones*	Secure development methodology; reinforcements R1 to R4 (where security testing is designed into the life cycle)	—	**R1–R4**	**R1–R4**	A at MEDIA, ALTA
Art. 31 *Auditoría de la seguridad*	Regular audit at least every two years; extraordinary audit after substantial changes. Sets the practical testing rhythm and the deadline for evidence	**Self-assessment**	**Certification**	**Certification**	A

Table 6.1 ENS Annex II measures that involve penetration or security testing, by category. "—" means the reinforcement is not required at that category. Identifiers are reproduced exactly as in Annex II of *Real Decreto 311/2022*.

Frequency

The ENS sets no numeric penetration-test frequency. It flows from the audit procedure (`[mp.s.2]` R1 says so expressly) and from the risk analysis; the Art. 31 two-year cycle and the extraordinary audit after substantial change set the practical rhythm. Section 6.3 turns this into a calendar.

Reading the identifiers

`[op.mon.3]` is the measure, `r6` the reinforcement and `.3` the item within it. Cite them exactly as written; certification auditors verify against CCN-STIC 808 item by item, and a paraphrased identifier costs time in the audit.

A · MANDATED — The legal text itself requires the test

B · REQUIRED BY SCHEME — Standard, scheme or own declared controls make it auditable

C · AUDITOR EXPECTATION — Not written; evidence expected in practice

D · RECOMMENDED — Good practice

6.3 Timing the test to the certification cycle

Months 1–18 · Operate	18	19–20	21–22	23	24
Continuous scanning ([op.mon.3] R2 at MEDIA and ALTA); vulnerability tracking and patching ([op.exp.4]); web-application audits before each release ([mp.s.2]); scoped test after any substantial change, which also triggers an extraordinary audit (Art. 31)	Scope and authorise the inspection	Penetration test, vulnerability analysis, configuration verification	Remediate to SLA; risk-accept the rest in writing	Retest; evidence pack	Art. 31 audit

Figure 6.2 A two-year ENS cycle planned backwards from the regular audit (Art. 31). The month numbers are a recommended plan (badge D); the two-year maximum interval and the extraordinary audit after substantial changes are the legal requirement (badge A).

Plan backwards from the audit date. A test finished six months before the audit leaves time for remediation, retest and an evidence pack the auditor can read without asking questions. A substantial change should trigger a scoped test before it goes live ([mp.sw.2], [op.exp.4] R1) and a note in the audit file, because it also triggers the extraordinary audit.

AUDITOR LENS

ENS auditors work from CCN-STIC 802 and 808 and look for the inspection report, the remediation record and the link to the risk analysis. A penetration-test report that does not state the category and the measures it evidences will be accepted, but only after the auditor has done that mapping; do it for them on the cover page.

SPAIN SPECIFIC · LANGUAGE

Certification bodies and contracting authorities work in Spanish. An English report is acceptable to most, but the executive summary and the measure mapping should be provided in Spanish; agree this in the rules of engagement.

6.4 Cloud providers: [op.nub.1]

A · MANDATED all categories

[op.nub.1] *Protección de servicios en la nube* (protection of cloud services) applies at every category. Under [op.nub.1.2], third-party cloud services must run on systems that are themselves ENS-conformant, or must meet a CCN-STIC guide (CCN-STIC 823, cloud services) whose requirements include, among others, "auditoría de pruebas de penetración (pentesting)". For a cloud or managed-service provider selling to the public sector this is the commercial reality: the customer's auditor will ask for the provider's ENS certificate at the relevant category, or for evidence against CCN-STIC 823 including penetration-test reports for the service.

6.5 Public-sector suppliers

A · MANDATED Art. 2 *Real Decreto 311/2022*

Art. 2 brings private providers into scope where their systems support public-sector services. *Ley 9/2017* (LCSP) contracts carry the ENS obligations into the supplier's contract, usually at the category of the contracting body's system, with a certificate or declaration due at award or within a stated period. Testing evidence ([mp.s.2] audits of the web applications delivered, [op.mon.3] inspections at ALTA) is then part of contract performance, not only of certification.

6.6 CCN-STIC guides the auditor will apply

GUIDE	SUBJECT	USE IN THE TESTING PROGRAMME
CCN-STIC 802	Audit of the ENS	The method the certification auditor follows; structure the evidence pack to its sections so each inspection finds its place.
CCN-STIC 808	Verification of compliance with the measures	Item-by-item check of Annex II; cite [op.mon.3.r6.3] and [mp.s.2] exactly on the report cover.
CCN-STIC 809	Declaration and certification of conformity	What the declaration (BÁSICA) and the certificate (MEDIA, ALTA) must state; what a supplier must be able to show a contracting authority.
CCN-STIC 817	Cyber-incident management	The path to follow, with CCN-CERT, if a test uncovers an actual compromise in a public-sector system.
CCN-STIC 823	Use of cloud services	The requirements a cloud provider evidences under [op.nub.1.2], including the penetration-testing audit.
CCN-STIC 825	ISO/IEC 27001:2022 and the ENS	Mapping to reuse ISMS evidence (8.8, 8.29) for ENS measures and vice versa when one programme serves both.

Table 6.2 CCN-STIC 800-series guides relevant to testing; cite number and version in force at the time of the test.

SECTION 7 NIS2

NIS2 in Spain: binding in substance, pending in law

Spain has not transposed NIS2. That changes who can enforce, not what the directive asks for, and one Implementing Regulation already applies without any Spanish act.

INSTRUMENT	STATUS AS AT 27 SEP 2026	DETAIL
Directive (EU) 2022/2555 (NIS2)	**Transposition deadline 17 October 2024 missed**	A directive binds Member States. The substance of Arts 20, 21 and 23 is fixed and is what the Spanish law must carry.
Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad	**Not enacted · not in the BOE · not in force**	Approved by the Council of Ministers at first reading on 14 January 2025. Would create the *Centro Nacional de Ciberseguridad* (CNC) as national coordinating authority and split supervision between the Ministry of the Interior, Defence (CCN) and Digital Transformation (INCIBE). No entry-into-force or transitional date is predicted in this report.
Infringement procedure INFR(2024)0270	**Reasoned opinion 7 May 2025; escalation continued in 2026**	Exact current stage to be verified before publication (Appendix 13.4).
Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024	**Directly applicable**	DNS service providers, TLD name registries, cloud computing, data centre and CDN providers, managed service providers, managed security service providers, online marketplaces, online search engines, social networking platforms and trust service providers. No Spanish act is needed (section 7.2).
Applicable Spanish NIS framework	***Real Decreto-ley 12/2018* and *Real Decreto 43/2021* (NIS1) remain in force**	Until the new law is in force. Reference CSIRTs: CCN-CERT (public sector), INCIBE-CERT (private sector and citizens), ESPDEF-CERT (defence).
NIS2 penalty regime	**Not enforceable in Spain**	Directive ceilings, mirrored in the draft: essential entities up to EUR 10 million or 2% of worldwide annual turnover; important entities up to EUR 7 million or 1.4%. Effective only once the national law is in force.

Status board Legal position as at 27 September 2026.

7.1 What binds in substance now

PROVISION	REQUIREMENT	TESTING RELEVANCE	BADGE
Art. 21(2)(e)	Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	Vulnerability-management process fed by testing; disclosure channel	B
Art. 21(2)(f)	Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	The provision under which penetration testing is expected; the policy must exist and be applied	B
Art. 20	Management bodies approve the risk-management measures, oversee their implementation, follow training and can be held liable	Board-approved testing programme; minutes; training record	B
Art. 23	Incident reporting: early warning within 24 hours, incident notification within 72 hours, final report within one month	A test that uncovers an actual compromise starts the clock; the rules of engagement must route it	B

LEGAL NOTE · WHY BADGE B

A directive is addressed to Member States and is not enforceable against a company in Spain until transposed. Badge B records that the directive is the reference text of the Spanish draft and of every customer and auditor questionnaire. Badge A is reserved for the directly applicable Implementing Regulation (page 18).

SCOPE OF THE DIRECTIVE

18 sectors: Annex I (high criticality) and Annex II (other critical sectors).

Medium-sized and large enterprises (50 or more staff, or turnover or balance sheet above EUR 10 million), plus listed exceptions regardless of size.

A · MANDATED
The legal text itself requires the test

B · REQUIRED BY SCHEME
Standard, scheme or own declared controls make it auditable

C · AUDITOR EXPECTATION
Not written; evidence expected in practice

D · RECOMMENDED
Good practice

7.2 Implementing Regulation (EU) 2024/2690: the mandate that already applies

Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 lays down the technical and methodological requirements of the Art. 21(2) measures for DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, online marketplaces, online search engines, social networking platforms and trust service providers. As a regulation it applies directly in Spain without transposition. Its Annex contains three points that a penetration-testing programme evidences.

LEGAL NOTE · SUPERVISION

The obligation is in force. Day-to-day supervision in Spain still depends on national authorities being designated by the transposition law; until then the supervisor's desk is not staffed by law, and enforcement pressure comes from customers, auditors and the Commission.

ANNEX POINT	REQUIREMENT	EVIDENCE THE PROGRAMME PRODUCES	BADGE
6.5 Security testing	A policy and procedures for security testing; the need, scope, frequency and type of tests determined; tests performed under a documented methodology; the policy reviewed at planned intervals. Penetration testing is the customary form of the test.	Security-testing policy; annual test plan with scope rationale; methodology statement (section 3.3); test reports; review minutes	A
6.10 Vulnerability handling and disclosure	Procedures to handle vulnerabilities in the entity's own products and services and to disclose them	Vulnerability-management procedure; disclosure channel; tracker linking each finding to its fix and retest	A
7 Assessing effectiveness	A policy and procedures to assess whether the cybersecurity risk-management measures are effectively implemented and maintained	Assessment policy; programme metrics; independent test results as evidence of effectiveness	A

Table 7.1 Testing-related points of the Annex to Implementing Regulation (EU) 2024/2690. Badge A applies to the entities listed above; other NIS2 entities should treat the same structure as badge D until the Spanish law specifies otherwise.

7.3 Management-body accountability (Art. 20)

Art. 20 makes the management body responsible for approving the cybersecurity risk-management measures, overseeing their implementation and following training, and allows it to be held liable for infringements as the national law will specify. For the testing programme this translates into four records:

1. **An approval paper**: the security-testing policy and the annual plan, approved by the board or its delegated committee and minuted.
2. **An oversight record**: results by severity and age, remediation against SLA and risk acceptances, presented at least twice a year.
3. **A training record** showing that members have followed training sufficient to understand the risks and the measures, including what a penetration-test report tells them.
4. **A decision trail** for anything left open: who accepted which risk, on what date, until when.

Under the Spanish draft the same duties fall on the *órgano de dirección* (management body); the vocabulary will settle on publication.

AUDITOR LENS

Point 6.5 is a policy test as much as a technical one. Assessors ask to see the document that determined need, scope, frequency and type before they open the report. A good report with no policy behind it evidences a test, not a control.

Keep the policy short, dated and reviewed at the interval it states.

A · MANDATED — The legal text itself requires the test

B · REQUIRED BY SCHEME — Standard, scheme or own declared controls make it auditable

C · AUDITOR EXPECTATION — Not written; evidence expected in practice

D · RECOMMENDED — Good practice

7.4 Building evidence before the law lands

1. **Record your scope position.** Sector against Annex I or Annex II, size against the threshold, exceptions checked; conclusion (essential, important or out of scope) dated and signed. Re-run it on publication.
2. **Adopt Art. 21(2) as the baseline.** For entities covered by Implementing Regulation (EU) 2024/2690, its Annex is the mandatory specification; for others it is the best available template (badge D).
3. **Write the security-testing policy in the shape of point 6.5**: need, scope, frequency, type, methodology, review interval. One page is enough.
4. **Run the programme in section 8** and keep the artefacts in Table 8.2 for every test.
5. **Stand up vulnerability handling and disclosure** (Art. 21(2)(e), point 6.10): intake channel, triage, SLAs, disclosure rules.
6. **Rehearse the Art. 23 clock.** Walk the path from a tester reporting an actual compromise to the 24-hour early warning, using today's CSIRT (INCIBE-CERT or CCN-CERT) and, where personal data is involved, the AEPD (GDPR Art. 33).
7. **Put it before the management body** (Art. 20): approve, minute, train.

LEGAL NOTE · PENALTIES

The directive's ceilings (essential entities: up to EUR 10 million or 2% of worldwide annual turnover; important entities: up to EUR 7 million or 1.4%) are mirrored in the Spanish draft. They cannot be applied in Spain until the national law is in force, and this report predicts no date.

SPAIN SPECIFIC

Nothing built against Arts 20, 21 and 23 is wasted when the law arrives: the draft transposes the directive's measures, and the evidence the future authorities will ask for is the evidence customers and auditors ask for today.

7.5 What changes on publication in the BOE

DIMENSION	TODAY (27 SEPTEMBER 2026)	AFTER THE LAW IS IN FORCE
Competent authority	None designated under NIS2; NIS1 authorities under *Real Decreto-ley 12/2018* and *Real Decreto 43/2021*	CNC as national coordinating authority; supervision by the Ministry of the Interior, Defence (CCN) and Digital Transformation (INCIBE), as enacted
Registration and notification duties	As under NIS1 for operators already designated	As the enacted law provides; do not assume the draft's text survives unchanged
Supervision	Customer and auditor driven; Commission pressure through INFR(2024)0270	Statutory supervisory and enforcement powers, as enacted
Penalties	Not enforceable	Up to the directive ceilings, as enacted
Penetration-testing badge	B Art. 21(2)(f) · A point 6.5 for Implementing Regulation entities	Expected to remain B unless the enacted text or its implementing rules name penetration testing; verify on publication
This report	Version 1.0	Re-issued: next review March 2027, or earlier on publication

Table 7.2 What the BOE publication of the Spanish NIS2 law changes for the testing programme, and what it does not.

A · MANDATED — The legal text itself requires the test

B · REQUIRED BY SCHEME — Standard, scheme or own declared controls make it auditable

C · AUDITOR EXPECTATION — Not written; evidence expected in practice

D · RECOMMENDED — Good practice

SECTION 8

One programme, four frameworks

Scope to the union of the four boundaries, test to one calendar, and produce each artefact once in a form every auditor recognises.

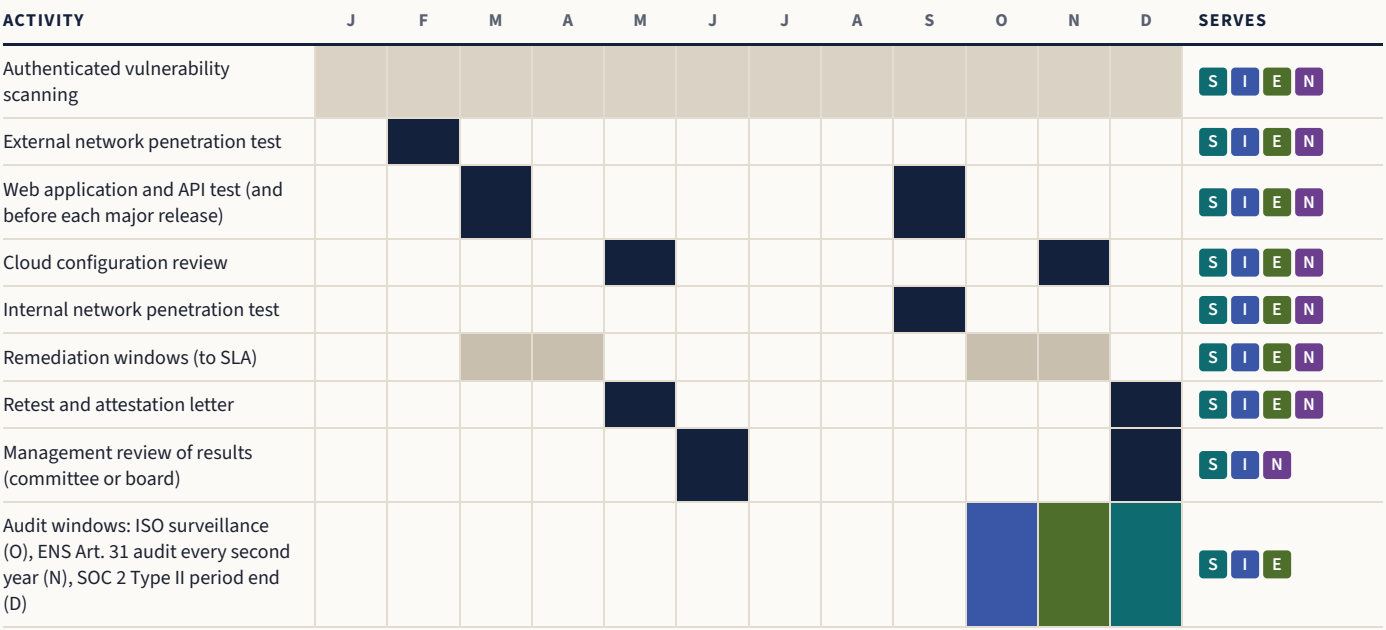


Figure 8.1 Unified annual testing calendar for a December year-end (recommended, badge D). Navy: testing and evidence events; sand: remediation windows; grey: continuous scanning; audit months in framework colour. S = SOC 2, I = ISO/IEC 27001, E = ENS, N = NIS2. Shift the whole calendar to your audit dates; keep the order.

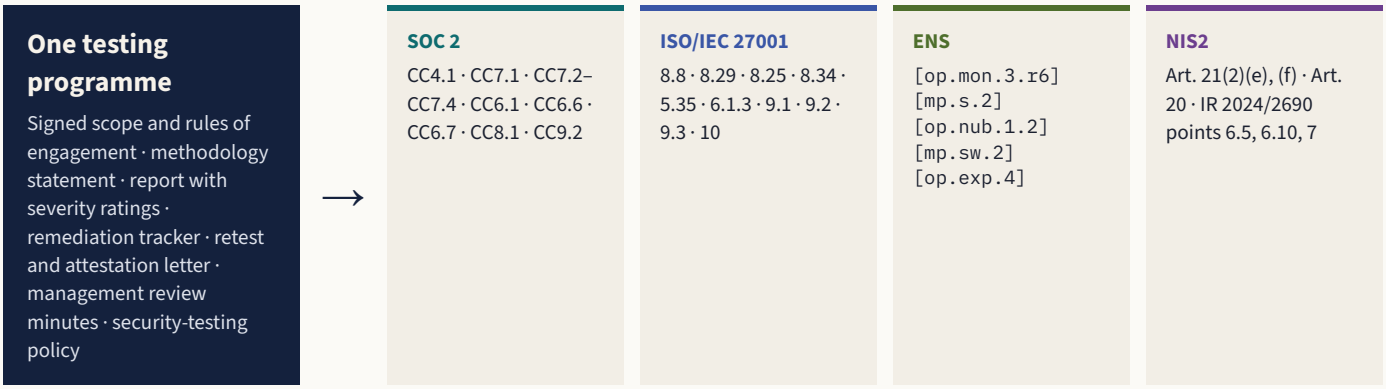


Figure 8.2 Test once, evidence four times: the same seven artefacts, filed against each framework's identifiers (detail in Table 8.2).

8.1 Scoping rules

1 · Start from the union of boundaries. SOC 2 system boundary, ISMS scope, ENS declaration of applicability and the systems supporting the NIS2 essential or important service. One inventory, tagged per framework.

2 · Test production-representative environments. Pre-production by default (ISO 8.31, ENS `[mp.sw.2]` R1); production only under the planning ISO 8.34 requires.

3 · Include third-party components you are entitled to test. Cloud and hosted assets under the provider's policy or written consent (section 9).

4 · Depth follows the strictest requirement in scope. ENS ALTA or an Implementing Regulation entity sets the floor for everyone sharing the system.

5 · Red team and TLPT supplement, never replace. Every framework accepts coverage testing; DORA Art. 26 adds TLPT for designated entities.

6 · Write down exclusions and why. Auditors read the exclusions first; an unjustified exclusion is an exception before the test starts.

8.2 Frequency matrix

ACTIVITY	SOC 2	ISO/IEC 27001	ENS	NIS2 · IR 2024/2690
External network test	At least one per review period C	Risk-based; annual expected C	Per audit procedure; before each Art. 31 audit and after substantial change; ALTA `[op.mon.3.r6.3]` A	Per own policy, point 6.5 A; Art. 21(2)(f) B
Web application and API test	Before significant releases (CC8.1) C	Before acceptance (8.29) C	`[mp.s.2]` during development and before production, continuous A	Art. 21(2)(e) B
Internal network test	Annual C	Risk-based C	ALTA `[op.mon.3.r6.3]`, periodically and after incidents A	Per own policy, point 6.5 A / B
Vulnerability scanning	Continuous or monthly (CC7.1) C	8.8 C	`[op.mon.3]` R2 at MEDIA and ALTA; `[op.exp.4]` A	Point 6.10 A; Art. 21(2)(e) B
Cloud configuration review	CC6.1, CC7.1 C	8.8 C	`[op.nub.1.2]`, all categories A	Point 6.5 A / B
Retest and closure	CC7.4 C	Clause 10 C	`[mp.s.2]` R2 findings fixed via `[op.exp.5]` A	Point 6.10 A / B
Red team / TLPT	D	D	D	D (DORA Art. 26: A every three years for designated financial entities)

Table 8.1 Frequency matrix. Where a cell shows two badges, the first applies to entities covered by Implementing Regulation (EU) 2024/2690 and the second to other NIS2 entities.

8.3 Cross-mapping: one artefact, four filing references

ARTEFACT PRODUCED	SOC 2	ISO/IEC 27001	ENS	NIS2 · IR 2024/2690
Signed scope and rules of engagement	CC4.1, CC9.2	8.34, 6.1.3	`[op.mon.3]` R6 · `[mp.s.2]` audit procedure	Point 6.5 (scope, type)
Methodology statement	CC4.1	8.29	`[mp.s.2]` R2 "defined methodologies"	Point 6.5 "documented methodology"
Final report with severity ratings	CC7.1, CC7.3	8.8	`[op.mon.3.r6.2]` · `[op.mon.3.r6.3]`	Points 6.5, 6.10
Remediation tracker	CC7.4, CC8.1	8.8, clause 10	`[op.exp.4]` · `[op.exp.5]`	Point 6.10
Retest report / attestation letter	CC7.4	8.8, 9.1	`[mp.sw.2]` acceptance criteria	Point 7
Management review minutes	CC4.1	9.3	Art. 31 audit file	Art. 20
Security-testing policy	CC4.1	5.36, 8.29	Audit procedure (`[mp.s.2]` R1 frequency)	Point 6.5

Table 8.2 Cross-mapping of artefacts to the identifiers each auditor files them under. Print the relevant row on each artefact's cover page.

A · MANDATED — The legal text itself requires the test

B · REQUIRED BY SCHEME — Standard, scheme or own declared controls make it auditable

C · AUDITOR EXPECTATION — Not written; evidence expected in practice

D · RECOMMENDED — Good practice

SECTION 9

Legal and contractual basis in Spain

A penetration test is, by construction, conduct the *Código Penal* describes as an offence. Written authorisation by the system owner is what makes it lawful, and everything else in this section protects that authorisation.

9.1 The Spanish authorisation basis

Código Penal	CONDUCT DESCRIBED	WHY IT MATTERS TO TESTING
Art. 197 bis	Unauthorised access to, or remaining in, an information system	Every test step is "access". The system owner's written authorisation is what takes the conduct outside the offence.
Art. 197 ter	Producing, acquiring or facilitating programs or credentials intended for those offences	The tester's toolkit. Authorisation and a documented purpose place its use inside a lawful engagement.
Arts 264–264 quater	Damage to data and interference with systems; tools for those offences; liability of legal persons for them	Denial-of-service, destructive payloads and data alteration must be excluded or tightly bounded in the rules of engagement.
Art. 31 bis	Corporate criminal liability of legal persons for offences committed for their benefit by representatives or employees	The commissioning company is exposed if a test exceeds its authority, for example against a supplier's system without consent.

The rules of engagement are therefore a legal instrument before they are a technical one. They must be signed by a person with authority over the systems, identify the assets, methods, windows and testers, and be in the testers' possession while they work. An oral agreement, a purchase order or an email chain does not meet that standard.

9.2 Third-party-hosted assets

Assets hosted by a third party need either the host's written consent or compliance with the host's published testing policy. Large cloud providers publish such policies, typically permitting tests of the customer's own resources without notice while prohibiting denial-of-service and tests against the provider's shared infrastructure; the policy's date and version belong in the rules of engagement. Testing a supplier's system, such as an outsourced application or a managed platform, needs that supplier's written consent, however strong the contractual right to audit.

9.3 Public-sector contracts

Ley 9/2017 (LCSP) governs public procurement. Contract clauses carry ENS obligations (Art. 2 of *Real Decreto 311/2022*) to suppliers. The contracting authority must authorise any test that touches its systems; the supplier's own systems supporting the service are within the ENS scope and are tested under the supplier's authorisation. Agree in the contract who tests what, who receives the reports and at which category.

LEGAL NOTE · WHO CAN AUTHORISE

The signatory must have actual authority over the system: the legal owner, or the operator under a contract that grants it. A project sponsor, a product manager or a reseller does not. Where systems are shared between group entities or joint-venture partners, obtain each owner's signature.

SPAIN SPECIFIC · IF A TEST FINDS A REAL COMPROMISE

The engagement becomes an incident. Route it through the incident procedure to the current CSIRT (INCIBE-CERT for the private sector, CCN-CERT for the public sector); to the AEPD within 72 hours where personal data is affected (GDPR Art. 33); and, for operators designated under *Real Decreto-ley 12/2018* and *Real Decreto 43/2021*, under that framework. The rules of engagement must name who makes the call.

AUDITOR LENS

ISO/IEC 27001 Annex A 8.34 asks that assurance activities on operational systems be planned and agreed with management. The signed rules of engagement are the evidence for that control as well as the legal basis.

9.4 Rules-of-engagement checklist

- ☐ Legal entity names of client and tester; signatories with authority over the systems
- ☐ Asset list: IP ranges, domains, applications, accounts, environments; explicit exclusions with reasons
- ☐ Test types and approach (black, grey, white box); exploitation limits; denial-of-service excluded
- ☐ Testing windows: dates, hours, time zone; blackout periods; change freeze interaction
- ☐ Tester source IP addresses; allow-listing and its removal after the test
- ☐ Points of contact and escalation path on both sides for the whole window
- ☐ Third-party systems: written consent or provider policy (date, version) attached
- ☐ Data handling: no extraction of real personal data; proof-of-access rules; redaction of screenshots
- ☐ Evidence storage location, encryption, access, retention period and destruction certificate
- ☐ Stop conditions; procedure and decision-maker if an actual compromise is discovered
- ☐ Reporting format, severity model (CVSS v4.0, EPSS, business context), retest scope and window
- ☐ Confidentiality (NDA), ownership of the report, permitted disclosure to auditors and authorities

9.5 Processor terms

When in-scope systems hold personal data, the tester processes it on the controller's behalf and GDPR Art. 28 applies: a written contract stating subject-matter, duration, nature and purpose of the processing, the types of data and categories of data subjects, and the processor's obligations (Art. 28(3)). Add minimisation (proof of access rather than extraction; no exfiltration of real personal data), an NDA, evidence handling (encrypted storage, access limited to the engagement team, redaction), retention and destruction with a certificate, and a duty to notify the controller without undue delay so that it can meet Art. 33. In Spain the *Ley Orgánica 3/2018* (LOPDGDD) applies alongside the GDPR and the AEPD supervises.

9.6 Cloud-provider rules

Attach the provider's testing policy (date, version) to the rules of engagement and confirm whether notification is required. Exclude the provider's shared infrastructure and any denial-of-service. For managed-service providers obtain written consent and agree who remediates what. Under ENS `[op.nub.1.2]` the provider should itself hold ENS conformity or CCN-STIC 823 evidence, including its own penetration-test audits; ask for it as part of due diligence (SOC 2 CC9.2, ISO/IEC 27001 supplier controls).

9.7 Evidence retention

FRAMEWORK	RETENTION DRIVER	RECOMMENDATION	BADGE
SOC 2	Auditors sample the current period and may ask for prior-period evidence; bridge letters refer to earlier reports	Keep reports, trackers and letters for at least three review periods	C
ISO/IEC 27001	Clause 7.5, documented information: control and retention of records	Retain through the three-year certification cycle	C
ENS	Art. 31 audit at least every two years; audit evidence under CCN-STIC 802	Retain at least two audit cycles (four years)	C
NIS2	Point 6.5 policy review at planned intervals; supervisory requests once authorities are designated	Retain per own policy, not less than three years	D
Raw evidence	Captures, credentials and extracted samples: GDPR minimisation and Art. 28 terms	Destroy within an agreed period after retest (for example 90 days), with a destruction certificate	D

Table 9.1 Retention of testing evidence. Reports and trackers are kept; raw evidence is destroyed.

A · MANDATED — The legal text itself requires the test

B · REQUIRED BY SCHEME — Standard, scheme or own declared controls make it auditable

C · AUDITOR EXPECTATION — Not written; evidence expected in practice

D · RECOMMENDED — Good practice

SECTION 10

Procuring a provider in Spain

The report is only as good as the people who write it and the terms under which they work. Buy named testers, documented independence and an audit-ready report, not a day rate.

10.1 Qualifications and certifications

Ask for the named testers, not the firm's brochure. Look for recognised offensive-security certifications held by the individuals who will do the work (for example OSCP or OSEP, CREST CRT or CCT, GIAC GPEN or GWAPT), a demonstrable track record in your test types, and, for ENS engagements, familiarity with CCN-STIC 802 and 808 and the ability to report in Spanish. For DORA threat-led testing, testers must meet Art. 27 and the requirements of Delegated Regulation (EU) 2025/1190.

10.2 Independence

The tester must not have built, operated or previously secured the system it tests, and must not be the ENS certification body or the SOC 2 service auditor of the same organisation. SOC 2 auditors expect an independent third party (badge C); ISO/IEC 27001 Annex A 5.35 asks for independent review; a certification body cannot audit its own testing. Rotate lead testers or firms every two to three years (badge D) and keep a signed conflict-of-interest declaration on file.

10.3 Insurance and liability

Require professional indemnity and cyber liability cover valid in Spain and proportionate to the systems in scope, and ask for the certificate rather than the promise. Liability clauses should allocate responsibility for damage within the rules of engagement to the provider and for damage caused by exceeding them to the party who exceeded them. A blanket exclusion of liability is a red flag.

10.4 Report-quality criteria

- [ ] Methodology standards named and followed
- [ ] Scope, exclusions and windows listed
- [ ] Every finding with evidence and reproduction steps
- [ ] CVSS v4.0 vector, EPSS and business-context rating per finding
- [ ] Mapping table to SOC 2, ISO/IEC 27001, ENS and NIS2 identifiers
- [ ] Remediation guidance specific to your stack
- [ ] Positive observations: controls that held, detection outcome
- [ ] Retest included and reported
- [ ] Executive summary a non-technical auditor can read
- [ ] Spanish executive summary and measure mapping for ENS

10.5 RED FLAGS

- Scan output relabelled as a penetration test
- No named testers, or no qualifications for the individuals
- No rules-of-engagement template of their own
- "Compliance guaranteed" or "certified pentest" claims
- Refusal to sign GDPR Art. 28 processor terms or an NDA
- Evidence stored outside the EU without a transfer basis (GDPR Chapter V)
- Fixed price offered without a scoping call
- Report delivered only as a tool export
- Retest not included in the price

10.6 Template RFP requirements

Twenty-one requirements to paste into a request for proposals. Each is a question the auditor will later ask you; make the provider answer it first.

A · SCOPE AND APPROACH

R-01 Confirm ability to test each listed asset class (external network, internal network, web application, API, cloud configuration on the named platforms) and state any you do not cover.

R-02 State the methodology standards followed per test type (OWASP WSTG, OWASP ASVS 5.0, PTES, NIST SP 800-115, OSSTMM) and provide the methodology document.

R-03 Propose the approach (black, grey or white box) per asset, with reasons.

R-04 Describe the severity model (CVSS v4.0 vectors, EPSS, business-context rating) with one worked example finding.

R-05 Explain how detection is tested and reported: whether the client's monitoring observed the testers.

B · TEAM

R-06 Name the lead tester and team, with individual qualifications and years of experience per test type.

R-07 Confirm that no team member has developed, operated or audited the systems in scope; provide a conflict-of-interest declaration.

R-08 Confirm reporting in English and Spanish, including a Spanish executive summary and ENS measure mapping.

C · LEGAL AND DATA PROTECTION

R-09 Provide the rules-of-engagement template, including signatory-authority requirements and stop conditions.

R-10 Accept GDPR Art. 28 processor terms; describe evidence handling, storage location, encryption, retention and destruction.

R-11 Confirm compliance with cloud providers' published testing policies and the process for third-party consents.

R-12 Provide certificates of professional indemnity and cyber liability insurance valid in Spain, with limits.

R-13 Describe the procedure if a test uncovers an actual compromise, including same-day notification to the client's named contact.

D · DELIVERABLES

R-14 Provide a redacted sample report showing executive summary, findings with evidence, remediation and mapping to SOC 2, ISO/IEC 27001, ENS and NIS2 identifiers.

R-15 Include retest of all Critical and High findings within the agreed window and an attestation letter (section 11).

R-16 Provide a technical debrief for engineering and a separate summary suitable for the management body (NIS2 Art. 20).

R-17 Deliver findings in a machine-readable format for import into the client's tracker.

E · COMMERCIAL

R-18 Quote a fixed price per scope item with day rates for additions; retest included.

R-19 Provide the delivery timeline: scoping, testing window, draft report, final report, retest.

R-20 Provide two references from clients in Spain in regulated sectors, with permission to contact.

F · EVALUATION

R-21 Recommended weighting (badge D): technical approach 35%, team 25%, deliverables and report quality 20%, legal and insurance 10%, price 10%. Price last, deliberately.

AUDITOR LENS

Keep the RFP, the winning response and the evaluation sheet. Together they evidence supplier due diligence (SOC 2 CC9.2) and the independence and competence of the tester, which every auditor checks before reading a single finding.

10.7 Evaluation sheet for R-21

CRITERION	WEIGHT	SCORED ON	FULL MARKS LOOK LIKE
Technical approach	35%	R-01 to R-05	A methodology document per test type; approach justified per asset; a worked severity example with CVSS v4.0 vector and EPSS; detection reporting described
Team	25%	R-06 to R-08	Named individuals with relevant certifications and years per test type; signed conflict-of-interest declaration; Spanish reporting capacity confirmed
Deliverables and report quality	20%	R-14 to R-17	Redacted sample meets the anatomy in section 11.1; retest and attestation letter included; management summary; machine-readable export
Legal and insurance	10%	R-09 to R-13	Own rules-of-engagement template; GDPR Art. 28 terms accepted; provider-policy compliance; insurance certificates supplied; compromise procedure documented
Price and delivery	10%	R-18 to R-20	Fixed price per scope item including retest; realistic timeline against the calendar in Figure 8.1; two Spanish regulated-sector references

Table 10.1 Evaluation sheet (badge D). Score each criterion 0 to 5, multiply by the weight, and keep the sheet: it is the supplier due-diligence record (SOC 2 CC9.2).

SECTION 11

Reporting

An audit-ready report answers the auditor's questions in the order they ask them: who authorised it, what was tested, how, what was found, what was fixed, and who was told.

11.1 Anatomy of an audit-ready report

1. **Document control.** Version, testing and issue dates, classification, distribution list, authorisation reference.
2. **Executive summary.** Scope in one paragraph, overall risk statement, findings by severity, three priority actions; readable without technical background.
3. **Scope and rules of engagement.** Assets tested, exclusions and reasons, windows, approach, source IPs, credentials used.
4. **Methodology.** Standards followed, phases, tool categories, limitations (time-boxed, rate-limited, environment).
5. **Findings.** Identifier, title, severity with CVSS v4.0 vector, EPSS, business-context rating, affected assets, evidence, reproduction steps, remediation, references (CWE).
6. **Detection and controls that held.** What monitoring saw (SOC 2 CC7.2, ISO 8.16) and which controls resisted exploitation.
7. **Remediation plan.** Owners, SLAs (Table 11.1), retest dates, risk acceptances pending.
8. **Retest results,** or a reference to the separate retest report and attestation letter (section 11.3).
9. **Appendices.** Framework mapping (one Table 8.2 row per artefact), tester qualifications, independence statement, Spanish summary for ENS.

Figure 11.1 Anatomy of an audit-ready penetration-test report, in the order auditors read it.

AUDITOR LENS

Auditors test the SLA you publish. Choose numbers you meet and document exceptions as risk acceptances signed by the owner, with an expiry date.

A missed SLA without a risk acceptance is an exception in SOC 2, a nonconformity in ISO/IEC 27001 and a finding in an ENS audit.

11.2 Remediation SLAs by severity

SEVERITY	MEANING (AFTER BUSINESS CONTEXT)	REMEDIATION TARGET	RETEST	GOVERNANCE
Critical	Actively exploitable; direct path to sensitive data or administrative control	Mitigate within 72 hours; fix within 7 days	Mandatory	Immediate escalation to the CISO; consider the incident procedure
High	Exploitable with moderate effort; significant impact on confidentiality, integrity or availability	30 days	Mandatory	Risk acceptance only by the risk owner, in writing, with expiry
Medium	Exploitable in combination with other weaknesses or under specific conditions	90 days	At next test	Tracked in the backlog with a named owner
Low	Limited impact; hardening and defence in depth	180 days or next major release	As needed	Batched into maintenance
Informational	No direct risk; observations and good-practice notes	No SLA	None	Recorded; reviewed at the next test

Table 11.1 Recommended remediation SLAs (badge D). None of the four frameworks fixes numeric SLAs; the numbers you publish in your policy become the standard you are audited against.

11.3 Retest

The retest closes the loop the auditor traces: finding, ticket, fix, verification. Retest every Critical and High finding within the SLA window, and record one of five statuses per finding. Deliver a short retest report or an addendum with the same identifiers as the original, then the attestation letter.

STATUS	MEANING AND REQUIRED EVIDENCE
Remediated	Retest could not reproduce the finding; the fix is described and the retest evidence attached.
Mitigated	Root cause remains; a compensating control reduces exploitability. Residual rating stated; permanent fix scheduled.
Risk accepted	Owner has accepted the risk in writing with justification and expiry date (ISO/IEC 27001 6.1.3; SOC 2 management assertion).
Open	Not yet fixed; still within SLA, or past SLA and flagged as an exception with escalation date.
Not retested	Outside the retest scope (usually Medium and below); reason recorded; verified at the next scheduled test.

11.4 Attestation letter

`Sample wording · on the provider's letterhead · one page`

Letter of attestation: penetration test

To the management of the Client. We confirm that, under the rules of engagement signed by both parties and referenced in our report, we performed a penetration test of the systems described in the attached scope statement during the agreed testing window. The test was carried out by the named team under the methodology set out in the report, based on OWASP WSTG, OWASP ASVS 5.0 and PTES, with severity assigned under CVSS v4.0 and the Client's business-context criteria.

The test identified the findings by severity stated in the report. We retested all findings rated Critical and High on the date stated in the retest report and confirm that each has been remediated or, where indicated, mitigated or formally risk-accepted by the Client.

We confirm that our firm and the individuals involved are independent of the Client and have not designed, built or operated the systems tested. This letter may be shared with the Client's auditors, certification bodies and competent authorities. It summarises and does not replace the full report.

Signed by the engagement lead and countersigned by a director of the provider, with date and report reference.

HOW EACH AUDITOR USES THE LETTER

SOC 2
Evidence that the control operated in the period (CC4.1) and that deficiencies were remediated (CC7.4).

ISO/IEC 27001
Sampled in internal audit (9.2) and presented at management review (9.3) as the 8.8 and 8.29 record.

ENS
Inspection evidence in the Art. 31 audit file, with the measure mapping (`[op.mon.3.r6.3]`, `[mp.s.2]`) on the cover.

NIS2
Record under Implementing Regulation point 6.5 and effectiveness evidence under point 7; summary for the management body (Art. 20).

AUDITOR LENS

The letter is a summary, never a substitute. Every auditor will ask for the full report, the tracker and the retest evidence; the letter's value is that it lets them file the engagement in one line before they do.

SECTION 12

Checklists and 90-day plan

Seven checks per framework. If every box is ticked, the next audit is a filing exercise; each unticked box is the exception the auditor will write.

SOC 2

- [ ] System description names penetration testing, its frequency and scope (moving the badge from C to B deliberately)
- [ ] Rules of engagement signed and dated within the review period
- [ ] Report dated within the period; testers named; independence statement on file
- [ ] Findings traced to tickets with owners and closure evidence (CC7.4, CC8.1)
- [ ] Retest report or attestation letter for all Critical and High findings
- [ ] Results minuted at the security committee (CC4.1)
- [ ] Sub-service organisations' reports reviewed and the review documented (CC9.2)

ISO/IEC 27001

- [ ] SoA entries for 8.8 and 8.29 state the implementing control and its frequency
- [ ] The testing procedure the SoA cites exists and matches practice
- [ ] Rules of engagement evidence the planning and agreement 8.34 requires
- [ ] Tests run in pre-production (8.31), or production testing planned under 8.34
- [ ] Findings feed the vulnerability register; control failures raised under clause 10
- [ ] Testing programme on the internal audit programme (9.2)
- [ ] Test metrics and open findings in the management review pack (9.3)

ENS

- [ ] Category and declaration of applicability confirmed; Table 6.1 measures identified for the system
- [ ] `[mp.s.2]` web-application audits during development and before production (R1 or R2; R2 + R3 at ALTA)
- [ ] At ALTA: `[op.mon.3.r6.1]` to `[op.mon.3.r6.3]` inspections performed periodically and after relevant incidents
- [ ] `[op.mon.3]` R2 dynamic analysis in place (MEDIA, ALTA)
- [ ] Cloud services evidenced under `[op.nub.1.2]` (ENS conformity or CCN-STIC 823 including pentesting audit)
- [ ] Test timing planned against the Art. 31 two-year audit and any substantial change
- [ ] Report carries the measure mapping and a Spanish executive summary

NIS2

- [ ] Scope position recorded: sector (Annex I or II), size, exceptions; Implementing Regulation (EU) 2024/2690 applicability checked
- [ ] Security-testing policy in the structure of point 6.5: need, scope, frequency, type, methodology, review
- [ ] Vulnerability handling and disclosure procedure (Art. 21(2)(e); point 6.10)
- [ ] Effectiveness-assessment record (Art. 21(2)(f); point 7) with test results attached
- [ ] Management-body approval, oversight minutes and training record (Art. 20)
- [ ] Art. 23 path rehearsed for a compromise discovered during testing (24 h, 72 h, one month)
- [ ] Watch item set for BOE publication of the transposition law; re-run this list on publication

12.1 Readiness checklist by framework. Items restate requirements from sections 4 to 7; badges as given there.

12.2 A 90-day plan

From a standing start to an audit-ready evidence pack in one quarter. Fifteen tasks, three phases, four frameworks served at once.

Days 1–30
FOUNDATIONS

01 Confirm the scope union: SOC 2 boundary, ISMS scope, ENS declaration, NIS2 service systems. One inventory, tagged per framework.

02 Adopt the security-testing policy in the point 6.5 structure and the severity model (CVSS v4.0, EPSS, business context).

03 Decide the SoA and system-description wording (sections 4.3 and 5.3); legal review.

04 Issue the RFP (section 10.6), select the provider, sign GDPR Art. 28 terms and the NDA.

05 Draft the rules of engagement; obtain owner signatures and third-party consents.

Outputs tagged inventory · policy v1.0 · signed rules of engagement · contract

Days 31–60
TEST

06 External network and web application/API tests in the agreed window.

07 Cloud configuration review; internal network test if in scope this cycle.

08 Detection check with the SOC: what did monitoring see, and when?

09 Triage findings within five working days; open tickets with owners and SLAs (Table 11.1).

10 Begin remediation of Critical and High findings; written risk acceptances where needed.

Outputs final report · remediation tracker · detection note

Days 61–90
EVIDENCE

11 Retest Critical and High findings; obtain the attestation letter (section 11.4).

12 Assemble the evidence pack: one Table 8.2 row per artefact; Spanish summary for ENS.

13 Present results to the management body; minute decisions (Art. 20, CC4.1, clause 9.3).

14 Update the SoA and system description to what was actually done.

15 Schedule the next cycle in the annual calendar (Figure 8.1); set the policy review date.

Outputs attestation letter · evidence pack · minutes · next-year calendar

Figure 12.1 The 90-day plan. Durations are recommendations (badge D); the legal requirements the plan serves are those cited in sections 4 to 7.

WHAT YOU HOLD AT DAY 90

SOC 2
A control statement and, in the period, the rules of engagement, report, tickets, retest letter and minutes it needs (CC4.1, CC7.1–CC7.4, CC8.1).

ISO/IEC 27001
SoA entries for 8.8 and 8.29 that match practice; 8.34 evidence; metrics for 9.1 and inputs for 9.2 and 9.3.

ENS
Inspection and web-application audit evidence mapped to `[op.mon.3]` and `[mp.s.2]`, timed to the Art. 31 cycle, with a Spanish summary.

NIS2
A point 6.5 policy, a point 6.10 procedure, effectiveness evidence under point 7 and Art. 20 minutes, ready for whichever authority the BOE eventually names.

ROLES AND DEPENDENCIES

TASKS	ACCOUNTABLE	RESPONSIBLE	CONSULTED	INFORMED
01–03 Scope and policy	CISO	GRC lead	Legal, DPO, service owners	Management body
04–05 Procurement and rules of engagement	CISO	Procurement, GRC lead	Legal, DPO, system owners, cloud and managed-service providers	Selected provider
06–10 Testing and triage	Head of engineering or IT operations	Provider, SOC, engineering leads	CISO, product owners	GRC lead
11–12 Retest and evidence pack	GRC lead	Provider, engineering	CISO, internal audit	Auditors, certification body
13–15 Governance and next cycle	Management body	CISO, GRC lead	Internal audit	Whole organisation

Risk: no signatory with authority
Rules of engagement stall in week 3. Identify system owners, including for shared and outsourced systems, in week 1.

Risk: remediation capacity
SLAs for High findings are missed in days 31–60. Ring-fence engineering time before the test starts, not after the report lands.

Risk: provider availability
The testing window slips past the audit date. Book the window at RFP award and make it a contractual milestone.

SECTION 13 · APPENDIX

13.1 Glossary

ENGLISH	SPANISH	MEANING IN THIS REPORT
Penetration test	*prueba de penetración, pentesting*	Authorised, methodology-led attempt to exploit weaknesses and demonstrate impact within an agreed scope.
Vulnerability scan	*análisis de vulnerabilidades*	Automated enumeration of known vulnerabilities and misconfigurations.
Red team, TLPT	*equipo rojo; pruebas de penetración basadas en amenazas*	Objective-based, intelligence-led adversary simulation; TLPT is the DORA Art. 26 form.
Rules of engagement	*reglas de compromiso; autorización de pruebas*	Signed authorisation defining assets, methods, windows, testers and stop conditions.
Statement of Applicability	*declaración de aplicabilidad*	ISO/IEC 27001 clause 6.1.3 document listing controls, justification and implementation.
System description	*descripción del sistema*	Management's description of the system in a SOC 2 report; the source of the controls tested.
Trust Services Criteria	*criterios de servicios de confianza*	AICPA TSP Section 100 criteria (2017, revised points of focus 2022).
Category (ENS)	*categoría del sistema*	BÁSICA, MEDIA or ALTA, by incident impact; determines the applicable measures and reinforcements.
Reinforcement	*refuerzo*	Additional requirement (R1, R2 …) within an ENS measure, required at a category or optional.
Declaration of conformity	*declaración de conformidad*	ENS self-assessment outcome permitted at category BÁSICA.
Certification of conformity	*certificación de conformidad*	ENS certificate issued by an ENAC-accredited body (MEDIA, ALTA).
Extraordinary audit	*auditoría extraordinaria*	ENS Art. 31 audit triggered by substantial changes to the system.
Essential, important entity	*entidad esencial, entidad importante*	NIS2 classification that drives supervision intensity and penalty ceilings.
Management body	*órgano de dirección*	Board or equivalent responsible under NIS2 Art. 20.
Implementing regulation	*reglamento de ejecución*	Directly applicable EU act detailing a directive's measures; here Implementing Regulation (EU) 2024/2690.
Transposition	*transposición*	National law giving effect to an EU directive; pending in Spain for NIS2 as at 27 September 2026.
CSIRT	*equipo de respuesta a incidentes de seguridad*	Incident response team: CCN-CERT, INCIBE-CERT, ESPDEF-CERT.
Processor	*encargado del tratamiento*	GDPR Art. 28 role of the tester when it processes personal data on the controller's behalf.
Risk acceptance	*aceptación del riesgo*	Documented decision by the risk owner to tolerate a finding, with justification and expiry.
Attestation letter	*carta de atestación*	Provider's signed summary of scope, method, results, retest and independence.
Security inspections	*inspecciones de seguridad*	ENS `[op.mon.3]` R6: configuration verification, vulnerability analysis and penetration tests.

13.2 References

EUROPEAN UNION LAW

Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2). Arts 20, 21(2)(e), 21(2)(f), 23; Annexes I and II.

Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures. Annex points 6.5, 6.10, 7.

Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector (DORA). Arts 24–27.

Commission Delegated Regulation (EU) 2025/1190 supplementing Regulation (EU) 2022/2554 with regard to regulatory technical standards on threat-led penetration testing (OJ 18 June 2025; applicable 8 July 2025).

Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act).

Regulation (EU) 2016/679 (General Data Protection Regulation). Arts 28, 32(1)(d), 33.

SPANISH LAW

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (BOE 4 May 2022). Consolidated text as amended by *Real Decreto 1125/2024*, with effect from 7 November 2024. Arts 2, 31; Annex II.

Real Decreto-ley 12/2018, de seguridad de las redes y sistemas de información; *Real Decreto 43/2021*, implementing it (Spain's NIS1 transposition).

Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad. Approved at first reading by the Council of Ministers, 14 January 2025. Not enacted as at 27 September 2026.

Ley Orgánica 10/1995, del Código Penal. Arts 31 bis, 197 bis, 197 ter, 264–264 quater.

Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

Ley 9/2017, de Contratos del Sector Público (LCSP).

Resolución de 13 de octubre de 2016: *Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad*.

Resolución de 27 de marzo de 2018: *Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información*.

STANDARDS AND ATTESTATION FRAMEWORKS

ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, with Amendment 1:2024. Clauses 6.1.3, 7.5, 9.1–9.3, 10; Annex A 5.35, 5.36, 7.1–7.14, 8.8, 8.16, 8.25, 8.26, 8.29, 8.31, 8.32, 8.34.

ISO/IEC 27002:2022, *Information security controls*. Guidance to 8.8.

AICPA, TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, with Revised Points of Focus (2022). CC4.1, CC6.1, CC6.6, CC6.7, CC7.1–CC7.4, CC8.1, CC9.2.

PCI Security Standards Council, *PCI DSS v4.0.1*, Requirement 11.4 (comparator only).

CCN-STIC GUIDES (CENTRO CRIPTOLÓGICO NACIONAL)

CCN-STIC 802, audit of the ENS · CCN-STIC 808, verification of compliance with ENS measures · CCN-STIC 809, declaration and certification of conformity with the ENS · CCN-STIC 817, cyber-incident management · CCN-STIC 823, use of cloud services · CCN-STIC 825, ISO/IEC 27001:2022 and ENS mapping. Cite the current version published by the CCN at the time of use.

METHODOLOGIES AND SCORING

OWASP Web Security Testing Guide (WSTG) · OWASP Application Security Verification Standard (ASVS) 5.0 · Penetration Testing Execution Standard (PTES) · NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment* · OSSTMM, *Open Source Security Testing Methodology Manual* · MITRE ATT&CK.

FIRST, *Common Vulnerability Scoring System v4.0* specification · FIRST, *Exploit Prediction Scoring System* (EPSS) · European Central Bank, *TIBER-EU Framework* (updated February 2025); TIBER-ES, Banco de España.

ENFORCEMENT RECORD

European Commission, infringement procedure INFR(2024)0270 against Spain for non-transposition of Directive (EU) 2022/2555: reasoned opinion 7 May 2025; escalation continued in 2026 (stage to verify, Appendix 13.4).

WHERE TO RETRIEVE THE OFFICIAL TEXTS

SOURCE GROUP	OFFICIAL REPOSITORY	CITATION PRACTICE
EU legislation	EUR-Lex, Publications Office of the European Union	Cite the Official Journal reference for the adopted text and the consolidated version's date when quoting an amended article.
Spanish legislation	*Boletín Oficial del Estado* (Agencia Estatal BOE)	Use the *texto consolidado* and record its last-updated date. The *Anteproyecto* is not in the BOE; it exists only as a Council of Ministers text.
CCN-STIC guides	CCN-CERT portal, *Centro Criptológico Nacional*	Guides are revised without renumbering; cite number, title and version or date.
ISO/IEC standards	ISO; in Spain through UNE, the national standardisation body	Licensed texts; cite edition year and amendment; quote clause and control numbers, not text.
AICPA criteria	AICPA & CIMA	TSP Section 100 (2017) with the 2022 revised points of focus; cite criterion identifiers (CC-series).
Methodologies and scoring	OWASP, PTES, NIST Computer Security Resource Center, ISECOM (OSSTMM), MITRE, FIRST, European Central Bank (TIBER-EU)	Freely published; cite version and retrieval date, as they change more often than legislation.

13.3 Regulatory watch list

ITEM	TRIGGER TO WATCH	EFFECT ON THIS REPORT
Spanish NIS2 transposition law	Publication in the BOE; entry into force; transitional provisions; designation of the CNC and sector supervisors	Re-issue: section 7, Table 1.1 and badges updated; next review brought forward
INFR(2024)0270	Referral to the Court of Justice, financial penalties or closure	Update section 2.1 and the status board on page 17
ENS Annex II	Any royal decree amending the measures of *Real Decreto 311/2022*	Update section 6 identifiers and Table 6.1
CCN-STIC 802, 808, 823, 825	New versions published by the CCN	Update references and audit-method notes in section 6
AICPA Trust Services Criteria	A new TSC edition or revised points of focus (none issued for 2025 or 2026)	Update section 4 and Table 4.1
DORA TLPT in Spain	TLPT-authority designations; TIBER-ES updates; supervisory designations of entities	Update section 2.5
Cyber Resilience Act	Delegated and implementing acts ahead of 11 December 2027	Update section 2.5 and the timeline
CVSS, EPSS, OWASP ASVS	New versions	Update sections 3.3 and 3.4

13.4 Assumptions and items to verify before publication

- Exact current stage of infringement procedure INFR(2024)0270 after the reasoned opinion of 7 May 2025.
- Current TLPT-authority designations in Spain under DORA and TIBER-ES before naming them.
- DORA Art. 25(1) as the provision listing penetration testing among test types (section 2.5).
- Cyber Resilience Act: Art. 14 as the manufacturers' reporting article; exact Annex I Part II point requiring regular security tests and reviews.
- ISO/IEC 27001:2022 Amd 1:2024 wording (climate-change considerations in clauses 4.1 and 4.2).
- Full official titles and dates of the Spanish instruments cited in 13.2, and the exact Spanish titles and current versions of CCN-STIC 802, 808, 809, 817, 823 and 825.
- PCI DSS v4.0.1 Requirement 11.4 sub-requirement wording (used as a comparator only).
- **Assumption:** no amendment to Annex II of *Real Decreto 311/2022* after *Real Decreto 1125/2024* as at 27 September 2026.
- **Assumption:** month numbers in Figures 6.2, 8.1 and 12.1 and the SLAs in Table 11.1 are recommendations, not legal deadlines.
- **Fact-base conflicts:** none identified. Where the authors' own knowledge differed from the fact base verified as at 27 September 2026, the fact base was followed.

13.5 Change log

VERSION	DATE	CHANGE
1.0	27 September 2026	Initial release. Legal position as at 27 September 2026.
Next review	March 2027	Or earlier if the Spanish NIS2 transposition law is published in the BOE.

DOCUMENT CONTROL

Title Penetration Testing for SOC 2, ISO 27001, ENS and NIS2 in Spain (2026)

Version 1.0 · 27 September 2026

Status Final; not legal advice (page 2)

Format A4 portrait, 32 pages, English (UK)

Publisher hacketico.es, a brand of Cyberscore B.V. (cyberscore.nl) · KVK-nummer 97451436