HORIZONSHIELD

Securing Your Digital Future, Today.

COMPLIANCE SERIES · BOOK 16 OF 16

Compliance & Audit Guide 2026

ISO 27001 · GDPR · NIS2 · SOC 2 · PCI-DSS — Complete Reference

Comprehensive guide to the major cybersecurity compliance frameworks: ISO 27001:2022, GDPR, NIS2, SOC 2 Type II, PCI-DSS v4.0, and DORA — with practical implementation, gap assessment, and audit preparation guidance.

FRAMEWORKS	CONTROLS	REGIONS	LEVEL
6	500+	EU/UK/US/Global	Practitioner

Contents

COMPLIANCE & AUDIT GUIDE 2026

01	Framework Overview — Which Applies to You?	OVERVIEW	4
02	ISO 27001:2022 — Implementation Guide	ISO 27001	8
03	GDPR Compliance Programme	GDPR	13
04	NIS2 Directive — Essential Entities	NIS2	17
05	SOC 2 Type II Readiness	SOC 2	21
06	PCI-DSS v4.0 — Requirements Overview	PCI-DSS	25
07	Audit Preparation & Evidence Management	AUDIT	29

CHAPTER 01

Compliance Framework Overview

Understanding which frameworks apply and how they overlap is the foundation of an efficient compliance programme.

ISO 27001 GDPR NIS2 SOC 2

Compliance Framework Selection Guide

Framework	Region	Who It Applies To	Certification/Audit	Max Penalty	Effective
ISO 27001:2022	Global	Any organisation (voluntary — but market-driven)	Third-party certification audit (annual surveillance + triennial full)	Reputational + contractual (no legal fine)	Current — 2022 revision supersedes 2013
GDPR	EU/UK	Processes EU or UK personal data — any organisation globally	Supervisory authority audit (complaint or proactive)	4% global annual turnover OR €20M (whichever higher)	May 2018 (UK: retained post-Brexit)
NIS2	EU	Essential and Important entities in 18 sectors	Supervisory authority — risk-based supervision	2% global annual turnover (Essential entities)	Jan 2023 — national implementation by Oct 2024
SOC 2 Type II	US (global adoption)	SaaS/cloud providers serving US	CPA firm audit (AT-C 205 standard)	Customer-driven — lose contracts without it	Ongoing — new criteria added regularly

Framework	Region	Who It Applies To	Certification/Audit	Max Penalty	Effective
		enterprise clients			
PCI-DSS v4.0	Global	Any entity processing, storing, or transmitting card data	QSA audit or SAQ (self-assessment)	Fines $5K-$100K/month + card processing suspension	v4.0 effective March 2024 (v3.2.1 EOL)
DORA	EU	Financial entities (see Book 04 for full scope)	National Competent Authority review	2% global turnover; criminal liability for board	Jan 17, 2025

Framework Overlap — Implement Once, Satisfy Many

Control Domain	ISO 27001 Reference	GDPR Article	NIS2 Article	SOC 2 Criteria	PCI-DSS Req.
Access control & IAM	A.8.1-A.8.7	Art. 32(1)(b)	Art. 21(2)(i)	CC6.1-CC6.3	Req. 7, 8
Incident management	A.5.24-A.5.28	Art. 33-34	Art. 23	CC7.3-CC7.5	Req. 10, 12.10
Risk management	Clause 6.1, A.6.1	Art. 35 (DPIA)	Art. 21(2)(a)	CC3.1-CC3.4	Req. 12.3
Cryptography	A.8.24	Art. 32(1)(a)	Art. 21(2)(h)	CC6.7	Req. 3, 4
Vulnerability management	A.8.8	Art. 32	Art. 21(2)(e)	CC7.1	Req. 11
Business continuity	A.5.29-A.5.30	Art. 32(1)(c)	Art. 21(2)(c)	A1.2-A1.3	Req. 12.4

UNIFIED CONTROL FRAMEWORK STRATEGY

Implement controls once to a high standard against the most demanding framework applicable to you. For EU companies: GDPR + ISO 27001 together cover ~80% of NIS2 requirements. Adding PCI-DSS adds encryption and network segmentation depth. A unified control framework with shared evidence collection dramatically reduces audit preparation costs.

CHAPTER 02

ISO 27001:2022 Implementation

ISO 27001 certification provides internationally recognised proof of your information security management system maturity.

ISMS | ANNEX A | CERTIFICATION | SURVEILLANCE

ISO 27001:2022 — Key Changes from 2013

The 2022 revision reorganised Annex A controls from 114 to **93 controls** in 4 themes (replacing 14 domains). 11 entirely new controls were added — most organisations working from 2013 mappings will have gaps.

New Control (ISO 27001:2022)	Reference	What It Requires	Common Gap
Threat intelligence	A.5.7	Collect and analyse relevant threat intelligence about your specific threats and vulnerabilities	No formal threat intel process — relying on reactive awareness only
Information security for cloud services	A.5.23	Specific policies and controls for cloud service use, consistent with cloud provider's security posture	Cloud-specific controls not addressed — covered under generic A.8.1 only
ICT readiness for business continuity	A.5.30	ICT must be explicitly addressed in BCDR planning and testing	BCP exists but ICT component not specifically documented or tested
Physical security monitoring	A.7.4	Continuous monitoring of physical premises where information is processed	CCTV/access logs not formally included in ISMS scope

New Control (ISO 27001:2022)	Reference	What It Requires	Common Gap
Configuration management	A.8.9	Documented, maintained, and reviewed security configurations for hardware, software, and services	No formal configuration baseline — ad hoc hardening
Information deletion	A.8.10	Controlled deletion of information when no longer needed, per retention policy	No formal data deletion process — data accumulates indefinitely
Data masking	A.8.11	Masking of sensitive data (PII, financial) in non-production environments	Production data used in development/test environments
Monitoring activities	A.8.16	Monitoring of systems, networks, and applications for anomalous behaviour	No SIEM or system monitoring — reactive only
Web filtering	A.8.23	Filtering of web access to manage risk of malicious content	No DNS/web filtering in place
Secure coding	A.8.28	Secure software development principles applied to in-house code	No secure coding standards or SAST/DAST in pipeline
Data leakage prevention	A.8.12	Technical controls to prevent unauthorised data exfiltration	No DLP solution or controls — data can leave undetected

ISMS Certification Roadmap

1

Gap Assessment (Month 1-2)

BASELINE

Assess current state against ISO 27001:2022 clauses 4-10 and all 93 Annex A controls. Document gaps. Define ISMS scope boundaries. Identify risk assessment methodology.

2

Risk Assessment & Treatment (Month 2-3)

FOUNDATION

Identify information assets, threats, and vulnerabilities. Produce risk register with treatment decisions. Map applicable Annex A controls to each risk. Produce Statement of Applicability (SoA).

3

Control Implementation (Month 3-8)

BUILD

Implement controls from SoA. Prioritise by risk. Document policies, procedures, technical controls, and evidence collection processes.

4

Internal Audit & PIR (Month 8-9)

VERIFY

Internal audit against all ISO 27001 clauses. Issue non-conformities. Management review meeting with documented outputs. Corrective action plan.

5

Stage 1 & Stage 2 Certification Audit (Month 10-11)

CERTIFY

Stage 1: Documentation review. Stage 2: On-site effectiveness audit. Successful completion → ISO 27001:2022 certificate (valid 3 years, annual surveillance audits).

CHAPTER 07

Audit Preparation

Certification audits are won or lost in the months before the auditor arrives.

EVIDENCE | CONTINUOUS COMPLIANCE | DOCUMENTATION | AUDIT TRAIL

Evidence Management Framework

Evidence Type	Examples	Retention	Format Standard	Common Failure
Policy documents	ISMS policy, AUP, password policy, incident management	3+ years — current version always available	Version-controlled, signed, dated, distribution list maintained	Outdated policies. No version control. Staff not acknowledged.
Risk register	Current risks, treatment decisions, residual risk ratings	All versions — full history	Dated, owner-assigned, reviewed minimum annually	Not reviewed annually. Risks never closed. No residual risk assessment.
Training records	Security awareness completion, role-based training	2 years minimum	LMS export or signed attendance records with date	Annual training not completed. No records for contractors/new joiners.
System configurations	Firewall rules, AD group policies, MFA config, encryption settings	Current + prior version + change record	Dated screenshots with admin login visible, or config export	No baseline configuration. Configuration changed without change record.

Evidence Type	Examples	Retention	Format Standard	Common Failure
Audit logs	SIEM alerts, access logs, privileged account activity, change logs	12 months minimum — often 24 months for compliance	SIEM export, timestamped, tamper-evident storage	Logs not retained. Only current logs available. No SIEM — manual review only.
Incident records	Incident log, investigation notes, post-incident reports	3 years minimum	Incident management system export, timestamped, root cause documented	No incident log. Incidents handled informally without documentation.
Penetration test reports	Annual pentest reports, vulnerability scan results, remediation status	Current + previous 2 years	Third-party report with remediation status tracking	No pentest performed. High findings unresolved at time of audit.

TOP CAUSES OF ISO 27001 CERTIFICATION FAILURE

(1) Policy-reality gap — documented procedures not followed in practice (auditors test both), (2) Incomplete training records — contractors and new joiners without documented training, (3) Stale risk register — risks not reviewed and updated at least annually, (4) Missing management review evidence — no documented formal ISMS governance meeting, (5) Undocumented changes — system changes without change management records, (6) SoA not maintained — Statement of Applicability not updated when controls added/removed, (7) Scope creep — new systems/services added without formal ISMS scope update.

CONTINUOUS COMPLIANCE TOOLS

Deploy automated evidence collection (Vanta, Drata, Sprinto, or Hyperproof) to automatically pull configuration evidence from cloud systems, MDM, HR systems, and CI/CD. Reduces audit preparation from 3 months of manual effort to 2 weeks of review. Provides year-round audit readiness and dramatically reduces cost per certification cycle.

HS

HORIZONSHIELD

Securing Your Digital Future, Today.

Compliance & Audit Guide 2026

Part of the HorizonShield Security Series — 16 comprehensive professional cybersecurity manuals covering every domain of modern enterprise security.