

Crossover Regulations

Navigating NIS 2, CRA, AMLR, DORA and eIDAS 2

Paloma Llaneza CerteIDAS

The Current Regulatory Framework

Regulation	Legal Basis	TSP Application	Supervisor	Key Dates	Penalties
NIS 2	Directive (EU) 2022/2555	Essential entity (Annex I)	Cybersecurity SB	Oct 2024 transposition	€10M or 2% turnover
CIR-NIS2	Reg (EU) 2024/2690	20-min threshold (Art. 14)	National CSIRT	7 Nov 2024 in force	As per NIS 2
DORA	Regulation (EU) 2022/2554	ICT third-party provider	ESAs (if critical)	17 Jan 2025	Per financial regulations
CRA	Regulation (EU) 2024/2847	Products with digital elements	Market surveillance	11 Dec 2027	€15M or 2.5% turnover
eIDAS 2	Regulation (EU) 2024/1183	Trust service providers	National SB	20 May 2024 in force	National implementation

Critical Issue: Each regulation creates distinct obligations for TSPs, with overlapping but non-harmonised requirements.

Commission Implementing Regulation (EU) 2024/2690

Article 14: Trust Service Providers - Specific Parameters

Critical incident

or more of the following criteria:

- (a) a trust service is **completely unavailable for more than 20 minutes**;
- (b) a trust service is **unavailable to users, or relying parties, for more than one hour calculated on a calendar week basis**;
- (c) **more than 1 %** of the users or relying parties in the Union, **or more than 200 000 users** or relying parties in the Union, whichever number is smaller, are impacted by limited availability of a trust service;
- (d) **physical access** to an area where network and information systems are located and to which access is restricted to trusted personnel of the trust service provider, or the protection of such physical access, is **compromised**;
- (e) the **integrity, confidentiality or authenticity of stored, transmitted or processed** data related to the provision of a trust service is compromised with an **impact on more than 0,1 % of users or relying parties**, or more than 100 of users or relying parties, whichever number is smaller, of the trust service in the Union.

Implications for TSP Operations

- Monitoring Granularity: Sub-minute detection capabilities required
- Incident Classification: Automated threshold detection systems
- Reporting Pipeline: 24-hour notification to CSIRT (not 72h as other entities)
- Key Management: Enhanced cryptographic material protection

Conflicting Requirements Analysis

Incident Reporting Timeline Conflicts

Framework	Initial	Detailed	Final	Authority
NIS 2 Art. 23	24 hours	72 hours	1 month	CSIRT + cybersec SB
eIDAS Art. 19(2)	Without undue delay	Within 24h (breach)	As appropriate	eIDAS SB
DORA Art. 19	Per RTS (4h major)	7 days	1 month	Lead overseer
GDPR Art. 33	72 hours	Without undue delay	As needed	DPA

Certification & Assessment Overlaps

Product Dimension (HSMs)

- CRA: CE marking + EU DoC
- eIDAS: QSCD certification (Art. 30)
- Common Criteria: EAL4+ evaluation

Service Dimension

- NIS 2: Security measures (Art. 21)
- eIDAS: Conformity assessment (Art. 20)
- DORA: ICT risk framework (if critical)

v2.3.1 (2021)

Pre-NIS2 baseline - ISO 27001/2 alignment

v3.1.1 (2024)

Initial NIS2 + Draft CIR-NIS2 mapping

v3.2.0 (2025)

Full CIR-NIS2 integration - DORA mapping

Technical Architecture

Core Standard

Clause 5: Risk Management
Clause 7: Security Controls
Clause 8: Assessment

Annex: DORA

ICT risk management mapping
5 pillars correlation
Financial sector alignment

Annex: NIS 2

CIR-NIS2 mapping

Technical Requirements Integration

Key Requirement Mappings in EN 319 401 v3.2.0

REQ-5-01 : Cybersecurity as integral part of TSP risk management

→ Satisfies: NIS 2 Art. 21(1), DORA Art. 5, ISO 27001:2022 Clause 6.1

REQ-7.9.1-01 : Continuous monitoring of security events

→ Enables: 20-minute detection (CIR-NIS2 Art. 14)

REQ-7.9.3-01 : Notification within 24 hours of breach identification

→ Harmonises: NIS 2, eIDAS, DORA reporting

REQ-7.8-17/18 : Annual penetration testing

→ Covers: DORA TLPT requirements, NIS 2 security testing

Proportionality Implementation

- REQ-4.2-01: Risk-based approach considering TSP size and exposure
- REQ-4.2-02: [PRO] markers for scalable requirements
- REQ-4.2-06: Maintained security posture regardless of size

Unified Assessment Architecture

EN 319 403 v3.1.1 - Requirements for CABs assessing TSPs

- Accreditation requirements (ISO/IEC 17065)
- Assessment methodology harmonisation
- Cross-regulation competence requirements

Assessment Consolidation Benefits

Traditional Approach	EN 319 403 Unified Approach
5 separate assessments	1 comprehensive assessment
Multiple CABs/auditors	Single accredited CAB
18-24 months total	6-9 months
Conflicting findings	Harmonised evaluation

DORA Integration: Annex A Deep Dive

Five Pillars Mapping

DORA Requirement	EN 319 401 Implementation	Evidence Generated
ICT Risk Management Arts. 5-16	Clause 5 + REQ-7.8	Risk register, control matrices
Incident Management Arts. 17-23	REQ-7.9.3-01 to 07	Incident logs, response procedures
Resilience Testing Arts. 24-27	REQ-7.8-13 to 19	Test reports, TLPT results
Third-party Risk Arts. 28-44	Clause 7.14	Vendor assessments, SLAs
Information Sharing Art. 45	Section 7.9.4	Threat intelligence feeds

Critical TSP Consideration: When designated as "critical ICT third-party provider" under DORA Art. 31, the EN 319 401 framework provides pre-validated compliance evidence for Lead Overseer review.

Products with Digital Elements - TSP Scope

In Scope

- Hardware Security Modules (HSMs)
- Signature creation devices
- Time-stamping units
- Certificate lifecycle management software

Requirements

- CE marking (Module B+C)
- 5-year vulnerability handling
- Software Bill of Materials
- Security by design documentation

EN 319 401 Alignment Strategy

Clause 7.14: Supply chain security

→ Addresses CRA when TSP is manufacturer AND user

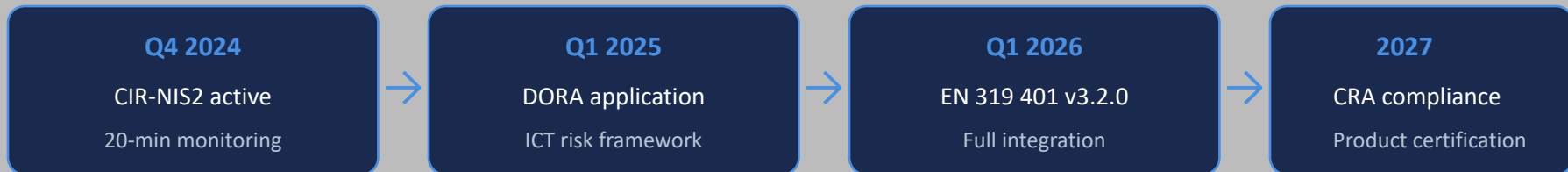
REQ-7.13: Vulnerability management

→ Exceeds CRA 5-year requirement with continuous process

REQ-7.8: Security testing

→ Generates evidence for CRA technical documentation

Regulatory Timeline vs Standard Evolution



TSP Action Items

- Immediate:** Implement 20-minute detection capability
- Q1 2025:** Align with EN 319 401 v3.1.1 framework
- Q1 2026:** Prepare for v3.2.1 assessment
- Ongoing:** Document compliance evidence for multi-regulation audit

Strategic timing: EN 319 401 v3.2.0 release in December 2025 provides 2 years preparation for CRA.

Monitoring & Detection Systems

REQ-7.9.1-01: Continuous monitoring implementation

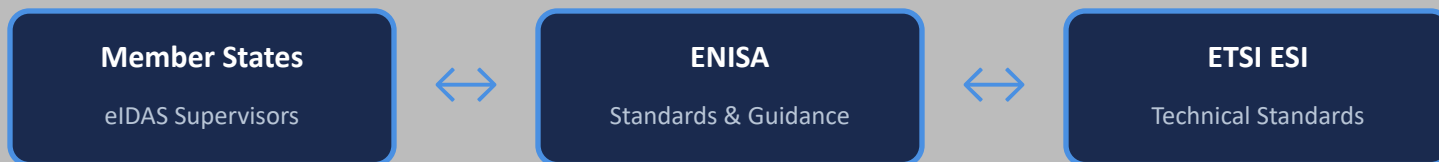
- Service availability: 1-minute granularity
- Key usage: Real-time cryptographic operations audit
- Integrity monitoring: Hash-chain verification
- Network traffic: Anomaly detection baseline

Incident Classification Matrix

Trigger	NIS 2	eIDAS	DORA	EN 319 401 REQ
Service down >20min	✓ Significant	✓ Notify	If financial	REQ-7.9.3-01
Key compromise	✓ Significant	✓ Immediate	✓ Major	REQ-7.9.3-02
25% integrity loss	✓ Significant	✓ Breach	If financial	REQ-7.9.3-03
€500K impact	✓ Significant	Assess	✓ Report	REQ-7.9.3-07

ENISA Coordination Framework Proposal

Governance Structure



Implementation Mechanisms

ENISA Role

- Coordinate MS implementation
- Publish unified guidance
- Facilitate supervisor cooperation
- Maintain incident taxonomy

Member State Actions

- Designate eIDAS SB as lead
- Adopt EN 319 401 framework
- Implement single reporting point
- Mutual recognition of assessments

Compliance Cost Comparison

Approach	Initial Assessment	Annual Maintenance	Re-certification	5-Year TCO
Fragmented (5 frameworks)	€800K-1.2M	€200K	€600K (year 3)	€2.6M
EN 319 401 Unified	€200-300K	€50K	€150K (year 3)	€650K
Savings	75%	75%	75%	€1.95M

Operational Benefits

- Single audit reduces operational disruption by 80%
- Unified evidence generation eliminates redundant documentation
- Consistent findings prevent conflicting remediation requirements

For SME TSPs, the unified approach means the difference between sustainable compliance and market exit.

Current Market Threats

Consolidation Drivers

- €200K per certification cycle
- 5+ parallel compliance tracks
- Specialist expertise shortage
- Conflicting requirements

At-Risk Segments

- Regional QTSPs (<50 employees)
- Specialised service providers
- Innovation-focused startups
- Non-qualified TSPs scaling up

EN 319 401 Proportionality Mechanisms

[PRO] Requirements: Scale with organisational capacity

Risk-based approach: Focus on actual threat landscape

Modular compliance: Core + service-specific requirements

Recognition framework: Leverage existing certifications

A diverse TSP ecosystem is essential for innovation, competition, and resilience in European digital infrastructure.

As EN 319 401 Editor - Key Insights

- Stakeholder alignment: 18 months of TSP community consultation
- Regulatory mapping with CIR-NIS2 and DORA
- CAB readiness: Training programme for assessors (EN 319 403)

Critical Success Factors

1. **Early engagement** with regulatory bodies (DG CONNECT, ENISA)
2. **Evidence-based** requirement development
3. **Backwards compatibility** with existing implementations
4. **Clear migration path** from v3.1.1 to v3.2.0

Outstanding Challenges

Member State transposition variations remain the primary risk to harmonisation.

Questions & Discussion

Contact for technical queries:

pllaneza@certicar.com

EN 319 401 v3.2.0 - Public draft available Q4 2025

EN 319 403 v3.1.1 - Published and available

ETSI TC ESI - Join the standardisation effort

Thank you