2026

seceon

DORA for the EU:
Turning Active Enforcement into a Growth Opportunity

How MSPs and MSSPs can help EU financial entities meet the Digital Operational Resilience Act's ICT risk, incident-reporting, testing, and third-party oversight requirements with our aiXDR Platform.

Executive Summary

The Digital Operational Resilience Act (DORA) is not a future deadline — it has applied directly across the EU financial sector since 17 January 2025. As an EU regulation rather than a directive, DORA required no national transposition: the same rules, the same reporting formats, and the same supervisory expectations apply from Lisbon to Warsaw the moment the application date passed.

2025 was largely a transition year, with supervisors assessing frameworks and building a picture of the sector's readiness. That grace period is over. 2026 is the year national competent authorities and the European Supervisory Authorities (EBA, ESMA, EIOPA) move from reviewing paperwork to active enforcement, cross-checking Register of Information submissions, running thematic reviews, and issuing the first formal remediation orders and penalty payments. Independent readiness surveys put full compliance at only around half of in-scope firms, which means a large share of the market is still exposed right as scrutiny intensifies.

For MSPs and MSSPs, this is a live, active-enforcement sales conversation, not a future one. DORA's third-party risk management pillar puts financial entities' own ICT vendors including MSPs and MSSPs directly inside the compliance picture, and firms that are behind need help now, not eventually.

> ***Why this matters now***
> *An estimated 22,000 financial entities and roughly 15,000 ICT service providers fall within DORA's enforcement perimeter. In November 2025, the ESAs designated the first 19 Critical ICT Third-Party Providers subject to direct EU oversight, including major cloud platforms a visible signal that enforcement has real teeth. With the second annual Register of Information cycle now underway across national portals, and only an estimated 50% of firms fully compliant, 2026 is the year DORA readiness stops being optional.*

This paper summarizes where DORA enforcement stands, what the regulation actually requires, who it affects, including MSPs and MSSPs themselves, and how our aiXDR Platform maps directly to its five pillars. It closes with a path for partners to package DORA readiness as a service. Sources consulted are listed in the Works Cited section on the final page.

1. Where DORA Stands Today

Already in force and now in active enforcement

DORA (Regulation (EU) 2022/2554) entered into force on 16 January 2023 and became fully applicable on 17 January 2025, after a two-year implementation window. Unlike NIS 2, DORA is a regulation, not a directive; it applies directly in every Member State without national transposition, which is why there is no French-, German-, or Irish-specific "DORA law" to wait for the way there is with NIS 2's Loi Résilience.

Supervisors treated 2025 largely as a baseline-assessment year. That has now changed. National competent authorities, such as the ECB, BaFin, ACPR, Banca d'Italia, the Central Bank of Ireland, and others, are conducting active enforcement reviews in 2026, cross-referencing Register of Information data automatically and moving toward formal penalties. The ECB has folded DORA findings directly into its Supervisory Review and Evaluation Process (SREP) for the roughly 113 significant credit institutions under its direct supervision — meaning weak ICT resilience can now translate into additional Pillar 2 capital requirements, not just a compliance finding.

A visible signal: Big Tech is now under direct EU oversight

On 18 November 2025, the EBA, EIOPA, and ESMA jointly published the first official list of Critical ICT Third-Party Providers (CTPPs), 19 providers, including major cloud infrastructure platforms, now subject to direct oversight by a designated Lead Overseer. This is the first mechanism giving EU authorities direct supervisory and penalty power over non-EU technology companies serving the European financial sector, and it signals that DORA's third-party oversight regime is operational, not theoretical.

How DORA relates to NIS 2 and GDPR

DORA functions as lex specialis for the financial sector: where DORA applies, Member States are directed not to separately apply NIS 2's cybersecurity risk-management, reporting, and supervision provisions to the same financial entities. In practice, this means financial entities that might otherwise be swept into NIS 2 as "important" or "essential" entities are instead governed by DORA's own broadly similar, but more prescriptive framework. For partners already positioning NIS 2 readiness, DORA is the natural adjacent conversation for any client in banking, insurance, payments, investment services, or crypto-asset services.

2. Who Is Affected — Including MSPs and MSSPs

A broad, intentionally inclusive scope

DORA applies to 20 categories of financial entities, including banks, insurers and reinsurers, investment firms, payment and e-money institutions, crypto-asset service providers, credit rating agencies, trading venues, and more, covering both established institutions and newer fintech models. The regulation applies proportionally: microenterprises (fewer than 10 employees and under €2 million turnover) qualify for a simplified ICT risk management framework under Articles 15–16, while larger and more systemically important entities face the full weight of the regulation, including threat-led penetration testing.

Critically, DORA's third-party risk management pillar extends the regulation's reach to ICT third-party service providers themselves, including MSPs and MSSPs serving financial-sector clients. A financial entity's DORA compliance is only as strong as its vendor oversight, which means its MSP/MSSP is now a direct input into the client's own regulatory risk, not just a service line item.

> ***The dual exposure***
> *An MSP/MSSP serving EU financial-sector clients sits inside DORA twice over: indirectly, as a vendor a client must now assess, contract, and monitor under Article 30's mandatory contractual provisions and the Register of Information; and directly, if designated a Critical ICT Third-Party Provider subject to EU-level oversight. Even without a CTPP designation, being demonstrably DORA-ready is quickly becoming a prerequisite to keep and win regulated financial-sector accounts.*

What non-compliance costs

DORA does not set a single EU-wide fine schedule for financial entities. Article 50 requires each Member State to establish its own effective, proportionate, and dissuasive penalties, so exact ceilings vary.

Most national regimes converge around fines of up to 2% of total annual worldwide turnover for financial entities, with several jurisdictions setting an additional floor around €10 million, and individual fines of up to €1 million for responsible senior managers. For designated Critical ICT Third-Party Providers, the EU-level penalty regime is more direct: the Lead Overseer can impose daily penalty payments of up to 1% of average daily worldwide turnover for continued non-compliance, for up to six months.

DORA also makes management-body accountability explicit: boards can be held personally liable for systemic failures in digital operational resilience, and several Member States allow criminal penalties for the most severe violations. As with NIS 2's Article 20, this turns operational resilience into a board-level agenda item rather than a purely technical one.

3. What DORA Actually Requires: The Five Pillars

DORA organizes its obligations into five pillars, each backed by detailed Regulatory and Implementing Technical Standards (RTS/ITS) from the European Supervisory Authorities.

Pillar 1 — ICT risk management

Financial entities must run a documented, board-owned ICT risk management framework covering identification, protection and prevention, detection, response and recovery, and continuous learning. The management body is explicitly accountable under Article 5; this is not a delegable IT function.

Pillar 2 — ICT-related incident reporting

DORA sets a strict, three-stage reporting clock for major ICT-related incidents once classified: initial notification within 4 hours of classification (and no later than 24 hours from detection), an intermediate report within 72 hours, and a final report within one month. The clock starts at classification, not detection — which makes fast, accurate classification itself a critical capability. Significant cyber threats can also be reported voluntarily to support sector-wide coordination.

Pillar 3 — Digital operational resilience testing

Entities must run a testing program that spans baseline testing (vulnerability scans, configuration reviews, failover drills, tabletop exercises) and, for entities designated by their competent authority, Threat-Led Penetration Testing (TLPT) aligned with the TIBER-EU framework. TLPT is the most operationally demanding element of DORA for the institutions in scope.

Pillar 4 — ICT third-party risk management

Financial entities must maintain a structured, continuously updated Register of Information (RoI) covering all ICT third-party arrangements provider details, contract scope, service locations, subcontractors, and criticality classification submitted annually and available for supervisory inspection at any time. Contracts with ICT providers must include mandatory provisions under Article 30 covering incident cooperation, audit rights, data location, and exit/substitution rights. This is consistently cited as the most operationally difficult DORA requirement: in the ESAs' 2024 dry-run exercise, only 6.5% of firms passed all 116 data-quality checks.

Pillar 5 — Information sharing

DORA permits, but does not mandate, voluntary sharing of cyber threat intelligence between financial entities to strengthen sector-wide resilience and situational awareness.

4. Our aiXDR Platform: Architecture, DORA Fit, and Economics

This section covers the engines behind the platform, a pillar-by-pillar mapping against DORA's requirements, the economics that matter to an MSP/MSSP serving financial-sector clients, and how aiCompliance CMX360 turns DORA's most burdensome pillar third-party and evidence management into an automated, recurring service.

4.1 Platform architecture at a glance

Our Open Threat Management (OTM) platform is built around a small number of core engines that ingest, correlate, and act on telemetry, rather than a bundle of loosely connected point products:

- aiSIEM — collects and analyzes logs and events from across the environment, using AI/ML rather than static correlation rules alone to identify anomalies and prioritize alerts.
- aiXDR — extends detection and automated response across endpoints, network, and cloud, correlating signals across domains to catch multi-stage attacks that any single tool would miss.
- SOAR — orchestrates and automates response workflows so that containment and remediation happen in seconds rather than waiting on manual analyst action critical when a 4-hour classification clock is running.
- UEBA — baselines normal user and entity behavior and flags deviations such as credential abuse, privilege escalation, and insider misuse.
- Dynamic Threat Models (DTM) — apply contextual, continuously updated risk scoring so alerts are prioritized by actual business risk, not just raw signal volume.
- aiCompliance CMX360 — the compliance engine, covered in detail in Section 4.5, that automatically maps existing security telemetry to controls across DORA, NIS 2, ISO 27001, and dozens of other frameworks.

We built this stack to replace the disconnected SIEM, XDR, SOAR, NDR, UEBA, and vulnerability-management tools many MSSPs previously had to license and integrate separately.

4.2 Pillar-by-pillar: DORA mapped to the platform

The table below maps each of DORA's five pillars to the platform capability that addresses it — the level of detail a partner needs when walking a financial-sector prospect's risk or compliance team through a gap assessment.

DORA Requirement	How the aiXDR Platform Delivers It
Pillar 1 — ICT Risk Management	Continuous, AI-driven visibility across endpoints, network, identities, and cloud provides a real-time view of organizational risk instead of a point-in-time assessment. Executive dashboards support Article 5 management-body accountability with actionable risk insights.
Pillar 2 — Incident Reporting (4h / 72h / 1-month)	aiXDR and SOAR automatically correlate, classify, and respond to security incidents as soon as they are detected. Comprehensive case timelines and audit trails enable analysts to compile regulator-ready documentation well within DORA reporting deadlines.
Pillar 3 — Resilience Testing (Including TLPT)	Continuous threat detection and Dynamic Threat Model (DTM)-based risk scoring provide the evidence required for Threat-Led Penetration Testing (TLPT), demonstrating control effectiveness through real operational telemetry rather than manually collected evidence.
Pillar 4 — ICT Third-Party Risk Management & the Register of Information (RoI)	aiCompliance CMX360 maps existing telemetry and security controls directly to DORA Register of Information (RoI) and Article 30 requirements, transforming third-party risk management from an annual compliance exercise into continuously maintained evidence.
Pillar 5 — Information Sharing	Multi-tenant architecture and standardized reporting enable MSSPs and financial institutions to securely aggregate anonymized threat intelligence across environments, supporting voluntary sector-wide information sharing and collaborative cyber resilience.

4.3 Built for MSP/MSSP economics, not just enterprise IT

Compliance mapping only matters commercially if a partner can deliver it profitably. Our own partner materials report onboarding of new client tenants in hours to days rather than weeks. One published case describes a global MSSP bringing its largest client fully onboard in four days, and prebuilt connectors, playbooks, and auto-tuning that cut onboarding time by up to 70%.

- Tool consolidation. We replace 10 to 20-plus siloed point tools with the unified OTM platform, reducing licensing overhead and the engineering effort of maintaining custom integrations between vendors.
- Partner economics. Partners running their own MSSP on our platform can target 60%-plus margins, or resell managed services with a guaranteed profit share of around 25%, alongside pricing that does not vary with data-volume growth.
- White-label delivery. Partners can present the platform under their own brand, branded portals, customized reporting, and partner-set pricing for MSPs/MSSPs that want to sell "their own" DORA readiness service rather than resell under our name.
- Flexible business models. Our platform supports MDR-as-a-Service, SIEM replacement/enhancement, and SOC-automation models side by side, so a partner can layer a DORA offer onto whichever delivery model it already runs.

4.4 Proof points from the field

Our partner materials cite production use across MSSPs and enterprises operating in regulated and multi-country environments, including financial-sector deployments. Examples include Exertis' "Fortress" managed security offering built on our platform, Exprivia's cybersecurity unit delivering AI/ML-driven, automated security operations across Europe on our platform, and an MSSP reporting the majority of its banking clients across Africa, including some of the region's largest institutions running on our platform. Partners are welcome to request direct reference customer introductions during due diligence.

4.5 Automating the third-party and evidence burden with aiCompliance CMX360

DORA's hardest pillar in practice is not incident response or testing, it's proving, continuously, that third-party ICT risk is managed and that evidence is ready for supervisors on demand. Only 6.5% of firms passed every data-quality check in the ESAs' own 2024 dry-run of the Register of Information, and independent research attributes much of that difficulty to scattered contracts, inconsistent vendor metadata, and unclear ownership across procurement, business units, and subsidiaries.

aiCompliance CMX360 is built to remove that manual burden by turning security data an organization already has into compliance evidence, rather than starting evidence-gathering from scratch. Because CMX360 sits directly on top of aiSIEM telemetry that's already being collected, it can reach 60–80% compliance readiness instantly across 20+ global and regional frameworks, including DORA, NIS 2, ISO 27001, GDPR, and Cyber Essentials, without a separate implementation project.

The workflow runs in three phases:

- Continuous ingestion. aiSIEM is already ingesting telemetry from every connected source, 24/7, as part of day-to-day security monitoring, not a separate compliance exercise layered on top.
- Automatic control mapping. The CMX360 engine maps that telemetry to the specific controls DORA and adjacent frameworks require, and keeps that mapping current as requirements and RTS/ITS updates change, rather than going stale between audits.
- Audit-ready reporting. CMX360 generates reports directly from that mapped evidence the same underlying evidence base that supports Register of Information submissions and supervisory inspection requests.

> ***What CMX360 changes***
> *Seceon reports that this combination cuts evidence-collection time by 90% and audit-completion time by 75%, and can compress SOC 2 readiness timelines from 6–9 months down to 2–3 weeks. For a partner that turns DORA compliance from a one-time project into a packaged, recurring service: a Compliance Readiness Assessment CMX360 scans the environment, maps controls, and produces a prioritized executive report that naturally leads into Continuous Compliance Monitoring, where CMX360 keeps validating controls, collecting audit evidence, and producing board-ready reports whenever a supervisor asks.*

Unlike a security project, a client might pause once complete. DORA's Register of Information is an annual, recurring filing obligation by design; the second cycle alone spans national deadlines through the first half of 2026. That makes CMX360-based compliance monitoring a natural fit for the subscription-based, recurring-revenue packaging outlined in Section 5.

5. Packaging DORA Readiness as a Partner Offering

DORA gives MSPs and MSSPs a rare combination: a regulation already in force, an active-enforcement year underway, and a client base including the partner's own financial-sector accounts with real exposure. Partners are best positioned to turn this into revenue by packaging readiness as a defined, sellable service rather than an open-ended consulting engagement.

5.1 A three-tier readiness offer built on one platform

Because the underlying platform is the same across all three tiers, partners can sell a land-and-expand motion starting with a fixed-scope assessment and growing the account into a full managed offering without re-platforming the client at any stage.

Service Tier	What's Included
Tier 1 — Assess	A fixed-scope DORA gap assessment across all five pillars, with a strong focus on the Register of Information (RoI) and Article 30 contractual requirements. Powered by aiCompliance CMX360, the assessment automatically maps existing controls, identifies compliance gaps, and delivers a prioritized remediation roadmap without the need for an extensive manual review.
Tier 2 — Monitor	Deployment and optimization of aiSIEM and aiXDR within the client's environment, with aiCompliance CMX360 continuously validating controls, collecting audit evidence, and tracking remediation progress. This provides the continuous compliance evidence required for the Register of Information and supervisory inspections.
Tier 3 — Respond & Report	A fully managed MDR/MSSP service combining SOAR-driven automated incident containment, support for DORA's 4-hour, 72-hour, and 1-month incident reporting requirements, and aiCompliance CMX360-generated executive and board-ready compliance reports to demonstrate management-body oversight and regulatory readiness.

5.2 A practical sequence for partner-led outreach

- Lead with the Register of Information. It is the pillar firms find hardest, and the one regulators are actively cross-checking in 2026 a natural, urgent entry point that doesn't require convincing a prospect that DORA applies to them.
- Make the assessment itself the demo. A CMX360-powered scan produces a mapped, prioritized findings report directly from the prospect's existing security data a concrete deliverable that does more to close a Tier 1 engagement than a slide deck.
- Position our platform as the control layer, not another tool. The value proposition is consolidation: one platform replacing the SIEM, XDR, SOAR, and UEBA point solutions clients would otherwise stitch together and separately justify to auditors and supervisors.
- Sell the reporting clock, not just detection. DORA's 4-hour classification window is unforgiving — frame our automated correlation and case timelines as the mechanism that keeps a client inside it.
- Address the board, not just the risk function. DORA's explicit management-body accountability, and its integration into the ECB's SREP process, is a natural hook for a briefing with the client's leadership team, not only its IT or risk function.
- Prove it on your own house first. Because MSPs/MSSPs sit inside DORA's third-party risk perimeter, a partner that can show its own DORA-aligned controls, running on our platform, has a credibility advantage that generic vendors cannot match.

> ***Cross-framework angle***
>
> *Because DORA functions as lex specialis for financial entities, partners already running NIS 2 conversations with non-financial clients can extend the same platform-based pitch to financial-sector accounts under DORA's parallel and in several respects more demanding framework, without retooling the underlying delivery model.*

DORA for the EU:
Turning Active Enforcement into a Growth Opportunity

The Scale of the Opportunity

22,000+
Financial entities in scope across the EU

2%
Max fine of global annual turnover

4 hrs
Window to classify a major ICT incident

Where DORA Stands

Jan 2023
Enters into force

Jan 2025
Fully applicable

Nov 2025
First 19 CTPPs named

2026
Active enforcement

H1 2026
2nd RoI cycle live

The problem

Reporting is too slow
Manual processes miss the 4-hour clock

RoI evidence is scattered
Only 6.5% pass every data check

MSPs are in scope too
Not just clients vendors are regulated

Boards face liability
Directors need risk visibility, not logs

DORA requires

Boards face liability
Directors need risk visibility, not logs

4h · 72h · 1-month
Tiered incident reporting to regulators

Board accountability
Management body must own ICT risk

Register of Information
Every vendor assessed, continuously

Seceon solves it

Auto-generated reports
SOAR files incident reports instantly

90% less audit effort
CMX360 maps controls automatically

Full-stack visibility
Endpoints, network, cloud, identity

Board-ready dashboards
Plain-language risk for leadership

90%
Evidence-collection time reduction

75%
Audit-completion time reduction

60-80%
Instant compliance readiness across 20+ frameworks

60%
Target MSSP margin on platform delivery

6. Frequently Asked Questions for Partners

"Isn't DORA just for large banks?"

No. DORA applies to 20 categories of financial entities, including payment institutions, e-money firms, investment firms, insurance intermediaries, and crypto-asset service providers, with proportionality provisions for smaller firms rather than an exemption. Even microenterprises face a simplified but real ICT risk management obligation under Articles 15–16.

"We've already done NIS 2 work with this client — isn't DORA redundant?"

Not for financial entities. DORA takes precedence over NIS 2 for in-scope financial entities, so NIS 2 readiness work doesn't automatically satisfy DORA's more prescriptive incident-reporting timelines, TLPT obligations, or Register of Information requirements. It's a related but distinct engagement on the same underlying platform.

"Is our MSP/MSSP itself really in DORA's scope?"

Indirectly, almost certainly, and potentially directly. Every financial-sector client's Article 30 contractual obligations and Register of Information now have to account for their MSP/MSSP as an ICT third-party provider. A small number of the largest providers are also directly designated as Critical ICT Third-Party Providers subject to EU-level oversight. 19 were named in the first designation round in November 2025.

"How fast can we actually get a client live?"

Our published partner accounts describe onboarding measured in hours to days rather than weeks, including a case where a global MSSP's largest client was fully onboarded in four days. Actual timelines vary by environment complexity and the state of a client's existing Register of Information partners should validate expected timelines with us directly during scoping.

"What if a client says they're already DORA-compliant?"

Worth testing that claim against the numbers: independent readiness surveys put full compliance at only around 50% of in-scope firms, and just 6.5% of firms passed every data-quality check in the ESAs' own dry-run of the Register of Information. "Compliant" and "has a policy document" are often two different things. A CMX360-powered gap assessment usually settles the question quickly, one way or the other.

7. Next Steps

DORA's grace period is over. With active enforcement underway, only around half of in-scope firms are fully compliant, and the Register of Information is now under direct supervisory scrutiny; financial entities and their ICT providers alike have a live, present-tense reason to act. Partners who help clients close that gap now, using a platform purpose-built for multi-tenant delivery and automated compliance evidence, will be the ones positioned to win the accounts that move first.

To discuss co-marketing this white paper, request a partner briefing deck, or scope a joint DORA readiness offer for your financial-sector client base, contact your Seceon partner representative or visit seceon.com.

About Seceon

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 850 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,800 clients.

References and Citations:

This whitepaper is based on research and data from:

- Digital Operational Resilience Act. Digital Operational Resilience Act (DORA). Available at: https://digital-operational-resilience-act.com
- European Insurance and Occupational Pensions Authority (EIOPA). Digital Operational Resilience Act (DORA). Available at: https://www.eiopa.europa.eu
- Legiscope. DORA Penalties and Enforcement: What to Expect. March 2026. Available at: https://legiscope.com
- Nemko Digital. DORA Compliance 2026: Key Requirements Explained. Available at: https://digital.nemko.com
- OrbiqHQ. DORA Compliance Guide 2026: Requirements & Deadlines. March 2026. Available at: https://orbiqhq.com
- Regulation DORA. DORA Penalties and Fines 2026: What Happens If You're Not Compliant? April 2026. Available at: https://regulation-dora.eu
- Seceon. How an MSSP Transformed Scaled Global Security Operations with Seceon. Available at: https://info.seceon.com

References and Citations:

- Seceon. Seceon aiCompliance CMX360: Instant, Security-Driven Compliance. Available at: https://seceon.com/aicompliance-cmx360/
- Seceon. Seceon Platform. Available at: https://seceon.com
- SureCloud. The 5 Pillars of DORA Explained. Available at: https://www.surecloud.com

About the Author

Shikha Pandey

Principal, Product Strategy & Partnerships, Seceon Inc.

Shikha leads Product Strategy, Global Marketing, and Partnerships at Seceon, where she drives go-to-market strategy, brand growth, channel expansion, and strategic partnerships. Before joining Seceon, she was a Senior Technical Program Manager at Meta, leading backend infrastructure programs supporting Facebook, WhatsApp, and Instagram, with a focus on automation, advanced tooling, and GenAI to improve engineering productivity.