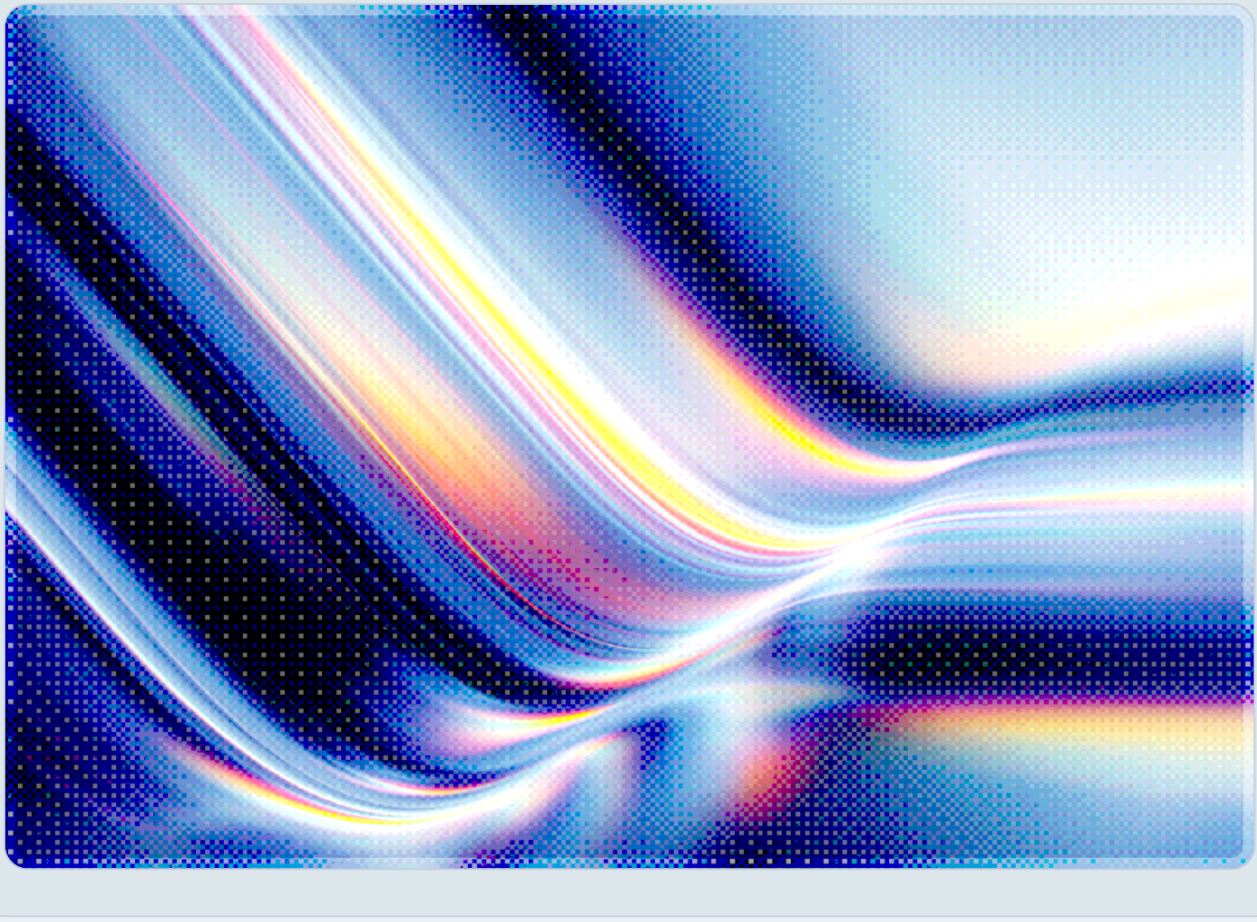
CSAI Foundation | Cloud Security Alliance

GDPR, NIS 2, and DORA Converge on Third-Party Risk

2026-08-22

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

- GDPR, NIS 2, and DORA now impose overlapping but independently enforceable obligations to assess, monitor, and remediate risk arising from vendors, processors, and ICT service providers, converting third-party oversight from a best practice into a compliance mandate with real financial exposure [1].
- Combined GDPR fines held at roughly €1.2 billion in 2025, and nearly a third of all documented GDPR enforcement actions to date cite failures under Articles 25 and 32 covering technical and organizational measures — a broad category that plausibly includes vendor oversight failures, since inadequate control over a processor's security measures falls within Article 28's scope [2][6].
- DORA's Register of Information requirement obligates in-scope financial entities to submit a complete inventory of ICT third-party contracts to national regulators by March 31, 2026, and the first cohort of 19 critical ICT third-party providers, including major cloud and technology vendors, is already under direct EU supervisory oversight [3][4].
- NIS 2 enforcement has moved from transposition to active supervision in 2026, with several member states beginning inspections that specifically test whether organizations can demonstrate systematic oversight of supplier security posture rather than point-in-time attestations [5].
- Most organizations still rely on manual, periodic vendor assessments that cannot keep pace with these continuous-monitoring obligations, leaving a structural gap between what the regulations require and what current third-party risk programs deliver — a diagnosis that draws substantially on CSA's own survey data [1].

Background

Three separate European regulatory regimes have arrived, within a span of a few years, at the same underlying conclusion: an organization's cybersecurity and data protection posture is inseparable from the posture of the vendors, processors, and service providers it relies on. The General Data Protection Regulation (GDPR) has enforced this principle since 2018 through Article 28, which holds data controllers liable when a processor fails to implement appropriate technical and organizational security measures, regardless of whether the controller's own systems were ever touched [6]. The Network and

Information Security Directive 2 (NIS 2), which EU member states were required to transpose by October 2024, extended a comparable logic to a much broader population of essential and important entities, mandating under Article 21 that organizations assess and manage risk in their supply chains and embed security requirements directly into supplier contracts [5]. The Digital Operational Resilience Act (DORA), fully applicable across the EU financial sector since January 17, 2025, went further still, establishing information and communication technology (ICT) third-party risk as one of its five core pillars alongside incident reporting, resilience testing, information sharing, and governance [3].

In CSA's assessment, what distinguishes the current moment from earlier compliance cycles is that all three regimes have now moved from legislative text to active enforcement, and their obligations increasingly point at the same underlying practice: continuous, evidence-based visibility into third-party security rather than static, calendar-driven questionnaires. CSA's own analysis of this convergence notes that organizations report spending roughly nine working weeks annually on vendor risk assessments while still experiencing vendor-related breaches, and that a majority of European firms believe their third-party providers carry meaningful compliance gaps that current assessment cycles fail to surface — a diagnosis that draws on CSA's own survey work rather than an independently audited, industry-wide dataset [1]. That gap is not merely an efficiency problem; under GDPR, NIS 2, and DORA alike, it is now a source of direct legal and financial exposure for the assessing organization, not just the vendor that fails.

The 2023 MOVEit Transfer breach illustrates why regulators converged on this issue. A single zero-day vulnerability in a widely used managed file transfer product cascaded into a breach campaign that, by early 2024, had compromised more than 2,700 downstream organizations and exposed data on more than 90 million individuals, generating remediation and legal costs that independent estimates place well into the billions of dollars [7][8]. In each case documented, the exposure arrived through a vendor relationship rather than a hole in the victim's own perimeter. Incidents of this kind, alongside a steady drumbeat of breaches attributed to compromised suppliers and managed service providers, illustrate why regulators have increasingly treated third-party oversight as a first-class compliance obligation rather than an implicit expectation buried inside broader security requirements.

Security Analysis

Where the Three Regimes Overlap

Despite differing origins and scopes, GDPR, NIS 2, and DORA converge on a common set of expectations: organizations must identify their material third parties, assess the risk each one poses, embed security obligations into contracts, monitor performance against those obligations on an ongoing

basis, and be able to demonstrate all of this to a supervisor on request. The table below summarizes how each regime frames that requirement and what happens when it is not met.

Regulation	Core Third-Party Obligation	Maximum Penalty	Enforcement Status (August 2026)
GDPR (Article 28)	Controllers must ensure processors implement appropriate security measures via binding contract; controller liability survives processor failure; 72-hour breach notification applies regardless of where in the chain a breach originated [6]	€20 million or 4% of global annual turnover, whichever is higher [1]	Mature; ~28% of all documented GDPR fines to date cite Article 25/32 technical and organizational measures failures — a broad category that plausibly includes vendor oversight gaps, since processor security failures fall within Article 28's scope [2][6]
NIS 2 (Article 21)	Essential and important entities must perform supply chain risk assessments, impose security criteria in supplier contracts, and manage incident reporting across downstream dependencies; senior management can face personal liability [5]	€10 million or 2% of global annual turnover [5]	Transposition largely complete; member states began active inspections and audits in 2026, with a January 2026 EU amendment narrowing scope for roughly 28,700 companies, including about 6,200 SMEs [5]
DORA	ICT third-party risk is a standalone pillar requiring a maintained Register of Information for every ICT contract, ongoing monitoring, exit strategies, and concentration risk management; critical	€5 million (or higher for individuals) for critical ICT third-party providers under direct oversight, plus periodic penalties of up to 1% of average daily worldwide	Fully applicable since January 17, 2025; Register of Information due to national competent authorities by March 31, 2026, reflecting data as of December 31, 2025; first 19 critical ICT third-party

Regulation	Core Third-Party Obligation	Maximum Penalty	Enforcement Status (August 2026)
	providers face direct EU supervision [3][4]	turnover for up to six months until compliance [3][9]	providers designated November 18, 2025 [3][9] [4]

Two features of this overlap deserve emphasis. First, liability under all three regimes attaches to the assessing organization, not solely to the vendor that fails. A controller cannot point to a processor's negligence as a defense under GDPR, an essential entity cannot point to a supplier's breach as a defense under NIS 2, and a financial entity cannot point to a critical ICT provider's outage as a defense under DORA. Each regime's liability structure has the effect of closing that escape route, regardless of whether foreclosing vendor-blame defenses was the drafters' primary intent. Second, all three impose a documentation and evidentiary burden that goes beyond having a policy on file. DORA's Register of Information must be submitted in a structured, machine-readable format to regulators annually, and NIS 2 supervisors are beginning to test not whether a contract contains a security clause but whether the organization can produce evidence that the clause is being monitored and enforced in practice [4][5].

Why Point-in-Time Assessment Fails Against These Requirements

The traditional third-party risk workflow, built around annual or biennial security questionnaires, a centralized vendor inventory maintained in a spreadsheet or generic GRC tool, and periodic contract review, was designed for a compliance environment where the underlying question was binary: does a control exist, yes or no. The regulations now in force ask a different question: is the control operating effectively, continuously, and can the organization prove it did so at the moment an incident occurred. A vendor that passed a security questionnaire in January and suffered a ransomware incident in July has, from the standpoint of NIS 2 or DORA, exposed the assessing organization to a supply chain risk that its assessment process failed to detect for six months. This is precisely the gap CSA's analysis of the convergence identifies: firms report that current assessment practices leave them unable to detect deteriorating vendor risk between review cycles, even as regulators increasingly treat that blind spot as a compliance failure rather than an unavoidable limitation [1].

The MOVEit incident again illustrates the mechanism. Organizations that had validated their MOVEit vendor's general security posture months earlier had no process capable of surfacing a zero-day disclosed after that assessment concluded, yet under GDPR's 72-hour notification clock and NIS 2's incident reporting obligations, they were required to respond as though continuous monitoring had been in place [6][7]. Concentration risk compounds this problem: DORA's explicit requirement that financial entities manage over-reliance on single ICT providers reflects regulators' recognition that when dozens

or hundreds of regulated entities depend on the same small set of hyperscale cloud and infrastructure providers, a single provider's failure or compromise can propagate systemically. That logic is consistent with the systemic risk the ESAs cited when designating the first cohort of critical ICT third-party providers, which includes several major cloud and technology vendors, for direct supervision [3][4].

Recommendations

Immediate Actions

Organizations subject to any of these three regimes should first confirm they have a single, authoritative inventory of third parties that maps cleanly to each regulation's scope: GDPR processors and sub-processors, NIS 2 supply chain dependencies, and, for financial entities, the ICT contractual arrangements that DORA's Register of Information requires. A vendor that appears in three disconnected spreadsheets maintained by procurement, legal, and security teams cannot be assessed consistently, and inconsistent internal records make it difficult to demonstrate the systematic oversight NIS 2 inspections are beginning to test for [5]. Financial entities in particular should treat the March 31, 2026, Register of Information deadline as a forcing function to reconcile these records now rather than in the final weeks before submission, since the register must reflect contractual data as of December 31, 2025, and inaccuracies discovered late are difficult to correct under a structured xBRL-CSV submission format [4].

Short-Term Mitigations

Programs should shift from static questionnaires toward a blended model that combines targeted point-in-time assessments for genuinely low-risk vendors with continuous, automated monitoring for vendors handling personal data, connecting to production systems, or falling within DORA's ICT third-party definition. This does not require replacing existing contracts wholesale; it requires amending renewal cycles to insert explicit monitoring, audit, and exit-strategy clauses consistent with what NIS 2 Article 21 and DORA both now expect contractually, and mapping each vendor's control evidence to more than one framework at once so that a single control validation satisfies GDPR, NIS 2, and DORA obligations simultaneously rather than requiring three parallel assessment tracks for the same vendor [1][3][5]. Security and privacy teams should also formally exercise breach notification playbooks that assume the initial compromise occurred inside a vendor's environment, since GDPR's 72-hour clock and NIS 2's reporting timelines both run regardless of where in the supply chain an incident originated [5][6].

Strategic Considerations

Over the medium term, organizations should treat concentration risk as a distinct governance question separate from individual vendor due diligence. The designation of 19 critical ICT third-party providers under DORA, several of which are cloud and infrastructure vendors used far beyond the financial sector, signals that regulators view dependency on a small number of dominant providers as a systemic exposure that individual contract terms cannot fully mitigate [3][4]. Boards and risk committees should ask not only "is this vendor secure" but "what is our organization's aggregate exposure if this vendor is unavailable or compromised," and should build exit strategies and provider-diversification options into strategic technology decisions rather than treating them as a compliance checkbox added after a vendor relationship is already operational. GDPR, NIS 2, and DORA enforcement is trending toward heavier scrutiny of documented, ongoing oversight rather than one-time attestations; in CSA's view, organizations that invest now in unified, continuously monitored third-party risk programs will be better positioned as additional EU digital regulations, and analogous frameworks emerging outside the EU, extend the same logic further.

CSA Resource Alignment

CSA's own research provides directly applicable guidance for the operational shift this convergence demands. The **Third-Party Vendor Risk Management** guide sets out a structured approach to assessing, scoring, and continuously monitoring vendor risk that maps closely to what NIS 2 Article 21 and DORA's ongoing-monitoring requirements now mandate; while framed around healthcare delivery organizations, its emphasis on near-real-time detection over static questionnaires is the same architectural shift this note recommends for any regulated entity. The **Healthcare Supply Chain Cybersecurity Risk Management** guide similarly demonstrates how to integrate supply chain risk into internal policy and formal supplier risk-rating processes, a pattern directly transferable to the contractual and documentation obligations under NIS 2 and DORA. CSA's earlier work, **From GDPR to California Privacy: Managing Cloud Vendor Risk**, addressed the GDPR-specific processor liability questions at the center of this note's Article 28 analysis and remains a useful primer on cross-jurisdictional vendor risk obligations, even as the regulatory landscape has since expanded well beyond GDPR alone. Finally, organizations building or maturing a unified control framework across these three regimes should reference the **AI Controls Matrix (AICM) v1.1**, which includes a dedicated third-party and vendor assessment questionnaire (AI-CAIQ) and role-based control guidance; while AICM is scoped to AI systems specifically, its structure for mapping shared-responsibility control ownership across model providers, service providers, and customers offers a reusable template for the kind of cross-framework control mapping this note recommends for GDPR, NIS 2, and DORA compliance more broadly.

References

[1] Cloud Security Alliance. "GDPR, NIS 2, and DORA Converge on One Problem: Third-Party Risk." CSA Blog, August 10, 2026.

[2] CMS Legal Services. "GDPR Enforcement Tracker Report, 6th Edition." CMS Law, May 2025.

[3] European Insurance and Occupational Pensions Authority. "European Supervisory Authorities Designate Critical ICT Third-Party Providers Under the Digital Operational Resilience Act." EIOPA, November 18, 2025.

[4] Regulation DORA. "DORA Register of Information: Complete Guide to the March 2026 Submission." Regulation-DORA.eu, 2026.

[5] 6clicks. "NIS2 Enforcement 2026: Critical Infrastructure, Government, and Defence Can't Wait." 6clicks, 2026.

[6] European Union. "Regulation (EU) 2016/679 (General Data Protection Regulation), Article 28." EUR-Lex, 2016.

[7] TechCrunch. "MOVEit, the Biggest Hack of the Year, by the Numbers." TechCrunch, August 25, 2023.

[8] Cybersecurity Dive. "Progress Software's MOVEit Meltdown: Uncovering the Fallout." Cybersecurity Dive, January 16, 2024.

[9] Bastion.tech. "DORA Timeline: Key Dates and Milestones." Bastion.tech, 2026.

