Seqlense

Cécile Henry
General Manager, CLR & Co-Founder

ESMA - Cyber risk and digital resilience as priorities for 2026

On 24 October 2025, the European Securities and Markets Authority (ESMA) published the news "Cyber risk and digital resilience will drive the agenda of ESMA's Union Strategic Supervisory Priorities for 2026"

ESMA has announced that from January 2025, it will treat **cyber risk and digital resilience** as a core Union-wide strategic supervisory priority (USSP) in the European Union financial markets. The priority is closely aligned with the application of the Digital Operational Resilience Act (DORA), which sets out regulatory requirements for firms' ICT risk management and digital operational resilience.

Since the launch of this priority, ESMA and national competent authorities (NCAs) have stepped up supervisory work—such as proactive checks, building supervisory capacity and monitoring firms' adherence to DORA-type requirements. ESMA emphasises that, in 2026, continued and reinforced efforts by NCAs and ESMA will be needed to ensure consistent and effective supervision across all EU jurisdictions, especially regarding group coordination and alignment with the DORA oversight framework.

In parallel, ESMA reminds that another USSP—ESG disclosures—remains active, with efforts in 2025 and 2026 to consolidate achievements and target high-risk areas. ESMA signals that, while cyber and digital resilience is the main new USSP, additional topics may be added to the supervisory agenda at the Union-wide level in future years.

Key points and implications

Cyber and ICT operational risk is now a central supervisory focus for ESMA across EU securities markets, not just a niche topic. The link to DORA means that firms subject to the ESMA's remit (or NCAs) must ensure they meet ICT risk management, incident reporting, testing, and resilience requirements. For regulated entities, this means stronger expectations around governance of ICT, business continuity, third-party risk, incident response, etc.

Cécile Henry
General Manager, CLR & Co-Founder

Regarding supervisory coordination and convergence across the EU, the interplay between DORA's framework and ESMA's USSP means firms must map not only local compliance but also their integration into group and/or infrastructure-wide digital resilience frameworks. These elements are also particularly important for cross-border firms, groups combining entities in different Member States, or firms using centralised services (shared infrastructure, third-party providers). ESMA calls on NCAs to coordinate their supervisory practices, monitor adherence to the digital resilience priority, and apply consistent supervisory treatment across jurisdictions.

The last key point concerns integration with other priorities, such as ESG disclosures, which are an existing USSP (since 2022), and ESMA expects work in 2026 to build on the progress made, notably in higher-risk areas. Firms should therefore be ready to face scrutiny not only on cyber and ICT risks but also on ESG disclosures, sustainable finance, and related areas. The dual track of digital resilience and ESG means firms need an integrated view of risk, including operational and ICT risks, digital transformation, data integrity, and ESG-related disclosures and controls.

<u>Sources :</u>

https://www.esma.europa.eu/press-news/esma-news/cyber-risk-and-digital-resilience-will-drive-agenda-esmas-union-strategic

Seqlense

Cécile Henry
General Manager, CLR & Co-Founder

ESMA - Le cyber-risque et la résilience numérique, priorités pour 2026

Le 24 octobre 2025, l'Autorité européenne des marchés financiers (ESMA) a publié l'information suivante : Le cyber-risque et la résilience numérique seront au cœur du programme des priorités stratégiques de surveillance de l'ESMA pour 2026 (“Cyber risk and digital resilience will drive the agenda of ESMA’s Union Strategic Supervisory Priorities for 2026”).

L'AEMF a annoncé que depuis janvier 2025, elle considère **les cyber-risques et la résilience numérique** comme une priorité stratégique de surveillance à l'échelle de l'Union (USSP) sur les marchés financiers de l'Union européenne. Cette priorité est étroitement liée à l'application de la loi sur la résilience opérationnelle numérique (DORA), qui définit les exigences réglementaires en matière de gestion des risques liés aux TIC et de résilience opérationnelle numérique des entreprises.

Depuis le lancement de cette priorité, l'ESMA et les autorités nationales compétentes (ANC) ont intensifié leur travail de surveillance, notamment par des contrôles proactifs, le renforcement des capacités de surveillance et le suivi du respect, par les entreprises, des exigences de type DORA. L'ESMA souligne qu'en 2026, les ANC et l'ESMA devront poursuivre et renforcer leurs efforts afin de garantir une surveillance cohérente et efficace dans toutes les juridictions de l'UE, en particulier en ce qui concerne la coordination au sein des groupes et l'alignement sur le cadre de surveillance DORA.

Parallèlement, l'ESMA rappelle qu'un autre USSP, celui des informations ESG, reste actif, avec des efforts en 2025 et 2026 visant à consolider les résultats obtenus et à cibler les domaines à haut risque. L'ESMA signale que, si la résilience cybernétique et numérique constitue le principal nouvel USSP, d'autres thèmes pourraient être ajoutés à l'agenda de surveillance de l'Union dans les années à venir.

Points clés et implications

Le risque opérationnel lié à la cybersécurité et aux TIC est désormais au centre des préoccupations de l'ESMA en matière de surveillance des marchés des valeurs mobilières

de l'UE et n'est plus un sujet de niche. Le lien avec la DORA signifie que les entreprises soumises à la compétence de l'ESMA (ou des ANC) doivent s'assurer qu'elles satisfont aux exigences en matière de gestion des risques liés aux TIC, de notification des incidents, de tests et de résilience. Pour les entités réglementées, cela se traduit par des attentes plus fortes en matière de gouvernance des TIC, de continuité des activités, de gestion des risques liés aux tiers, de réponse aux incidents, etc.

En ce qui concerne la coordination et la convergence de la surveillance dans l'UE, l'interaction entre le cadre DORA et l'USSP de l'ESMA implique que les entreprises doivent non seulement se conformer aux exigences locales, mais aussi s'intégrer aux cadres de résilience numérique à l'échelle du groupe et/ou de l'infrastructure. Ces éléments sont également particulièrement importants pour les entreprises transfrontalières, les groupes regroupant des entités dans différents États membres, ainsi que pour les entreprises utilisant des services centralisés (infrastructure partagée, fournisseurs tiers). L'ESMA invite les autorités nationales compétentes à coordonner leurs pratiques de surveillance, à contrôler le respect de la priorité accordée à la résilience numérique et à appliquer un traitement de surveillance cohérent dans toutes les juridictions.

Le dernier point clé concerne l'intégration avec d'autres priorités, telles que les informations ESG, qui font partie de l'USSP (depuis 2022), et l'ESMA prévoit que les travaux menés en 2026 s'appuieront sur les progrès réalisés, notamment dans les domaines à haut risque. Les entreprises doivent donc être prêtes à faire l'objet d'un examen minutieux non seulement des risques cybernétiques et informatiques, mais aussi des informations ESG, de la finance durable et des domaines connexes. La double voie de la résilience numérique et de l'ESG implique que les entreprises ont besoin d'une vision intégrée des risques, y compris les risques opérationnels et informatiques, la transformation numérique, l'intégrité des données, ainsi que les informations et contrôles liés à l'ESG.

Sources :
https://www.esma.europa.eu/press-news/esma-news/cyber-risk-and-digital-resilience-will-drive-agenda-esmas-union-strategic