Seqlense

Cécile Henry
General Manager, CLR & Co-Founder

ESAs designate critical ICT third-party providers under DORA

Under the Digital Operational Resilience Act (DORA), the European Supervisory Authorities (ESAs), comprising the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA), have published a list of critical ICT third-party providers (CTPPs) that will be placed under direct supervision by the European authorities, with the support of national authorities.

This represents an important step in deploying the supervision framework for digital operational resilience within the financial industry. The procedure adhered to the DORA methodology: data collection, criticality assessment in collaboration with national competent authorities, notification of providers entitled to be heard, and the ultimate designation. The designated CTPPs deliver essential infrastructure or business and data services to EU financial institutions. The objective of the oversight framework is to ensure robust ICT risk management and governance by these providers, thereby enhancing the operational resilience of the financial sector.

Main Key Points

This announcement made by the ESAs highlights that they have issued the list of critical ICT third-party providers (CTPPs) and that these providers are now subject to direct supervision under DORA. National regulators, including the ACPR, will support this governance framework for the providers. The objective is to strengthen the sector's operational resilience by ensuring that these providers (which deliver critical IT services) are appropriately overseen, as their failure or impairment could have systemic consequences.

The ESAs used data from registers of information maintained by financial entities, detailing their contractual arrangements for ICT services. The assessment of criticality was conducted in accordance with several criteria delineated within DORA, including systemic significance, contribution to essential functions, and the feasibility of service substitution.

Seqlense

Cécile Henry
General Manager, CLR & Co-Founder

Following the evaluation, the providers identified as critical were officially informed. They granted the opportunity to submit a reasoned statement (the "right to be heard"), before the issuance of a definitive designation decision. The scope of services rendered by designated CTPPs is extensive, encompassing essential ICT infrastructure, business, and data services, and includes financial entities of all types and sizes within the European Union. The primary aim of oversight is to foster effective governance of ICT risks by these providers through direct supervisory engagement conducted by the ESAs. This part of the DORA implementation marks a step towards operational resilience in the financial sector.

Conclusion

DORA appears to be transitioning from a conceptual framework to a practical application. The designation of critical ICT third-party providers represents a tangible measure of this evolution. The oversight is straightforward for these providers, requiring them to adhere to governance, risk management, incident reporting, and other obligations. At the same time, financial institutions must oversee and manage their interactions with them.

For entities such as CASPs, particularly when incorporated into crypto-asset platforms and broader financial services, it indicates heightened expectations regarding ICT and third-party risk management.

Sources :

- https://acpr.banque-france.fr/fr/actualites/nouvelle-etape-dans-la-mise-en-oeuvre-de-dora
- https://www.esma.europa.eu/press-news/esma-news/european-supervisory-authorities-designate-critical-ict-third-party-providers

Seqlense

Cécile Henry
General Manager, CLR & Co-Founder

Les AES désignent les fournisseurs tiers de TIC essentiels au titre de la DORA

En vertu de la loi sur la résilience opérationnelle numérique (DORA), les autorités européennes de surveillance (AES), qui comprennent l'Autorité bancaire européenne (EBA), l'Autorité européenne des assurances et des pensions professionnelles (EIOPA) et l'Autorité européenne des marchés financiers (ESMA), ont publié une liste des fournisseurs tiers essentiels de TIC (CTPP) qui seront placés sous la supervision directe des autorités européennes, avec le soutien des autorités nationales.

Il s'agit d'une étape importante dans la mise en place du cadre de supervision de la résilience opérationnelle numérique dans le secteur financier. La procédure a respecté la méthodologie DORA : collecte de données, évaluation de la criticité en collaboration avec les autorités nationales compétentes, notification des fournisseurs ayant le droit d'être entendus et désignation finale. Les CTPP désignés fournissent des infrastructures ou des services commerciaux, ainsi que des données essentielles aux institutions financières de l'UE. L'objectif du cadre de surveillance est de garantir, par ces fournisseurs, une gestion et une gouvernance solides des risques liés aux TIC, renforçant ainsi la résilience opérationnelle du secteur financier.

Points clés

Cette annonce, faite par les AES, met en avant la publication de la liste des fournisseurs tiers de TIC critiques (CTPP) et indique que ces fournisseurs sont désormais soumis à une surveillance directe dans le cadre de la DORA. Les régulateurs nationaux, dont l'ACPR, soutiendront ce cadre de gouvernance pour les fournisseurs. L'objectif est de renforcer la résilience opérationnelle du secteur en veillant à ce que ces fournisseurs (qui prennent en charge des services informatiques critiques) soient correctement surveillés, car leur défaillance ou leur dégradation pourrait avoir des conséquences systémiques.

Les AES ont utilisé les données issues des registres d'informations tenus par les entités financières, qui détaillent leurs accords contractuels pour les services TIC. L'évaluation de la criticité a été réalisée conformément à plusieurs critères définis dans DORA, notamment l'importance systémique, la contribution aux fonctions essentielles et la faisabilité de la

Cécile Henry
General Manager, CLR & Co-Founder

substitution des services. À l'issue de l'évaluation, les fournisseurs identifiés comme critiques ont été officiellement informés. Ils ont eu la possibilité de présenter un exposé motivé (le « droit d'être entendu ») avant la publication d'une décision de désignation définitive. L'étendue des services fournis par les CTPP désignés est vaste, couvrant les infrastructures TIC essentielles, les services commerciaux et les services de données, et incluant les entités financières de tous types et de toutes tailles au sein de l'Union européenne. L'objectif principal de la surveillance est de favoriser, auprès de ces fournisseurs, une gouvernance efficace des risques liés aux TIC grâce à une supervision directe exercée par les AES. Cette étape de la mise en œuvre de DORA marque une étape vers la résilience opérationnelle dans le secteur financier.

Conclusion

La DORA semble passer d'un cadre conceptuel à une application pratique. La désignation des fournisseurs tiers de TIC critiques constitue une mesure tangible de cette évolution. La surveillance est simple pour ces fournisseurs, qui sont tenus de respecter des obligations en matière de gouvernance, de gestion des risques, de signalement des incidents, entre autres. Parallèlement, les institutions financières doivent superviser et gérer leurs interactions avec eux.

Pour les entités telles que les CASP, en particulier lorsqu'elles sont intégrées à des plateformes de crypto-actifs et à des services financiers plus larges, cela traduit des attentes accrues en matière de TIC et de gestion des risques liés aux tiers.

Sources :
· https://acpr.banque-france.fr/fr/actualites/nouvelle-etape-dans-la-mise-en-oeuvre-de-dora
· https://www.esma.europa.eu/press-news/esma-news/european-supervisory-authorities-designate-critical-ict-third-party-providers