TRANSPOSITION DE DORA

QUESTIONNAIRE DE LA COMMISSION SPÉCIALE DE L'ASSEMBLÉE NATIONALE

Réponse de l'AMAFI

Une commission spéciale de l'Assemblée nationale prévoit l'examen, à l'automne 2025, du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, dont le titre III est consacré à la transposition la directive DORA (*directive (UE) 2022/2556*).

M. Mickaël Bouloux, député d'Ille-et-Vilaine (8e circonscription), rapporteur de ce titre III, a entendu les représentants du secteur financier, au cours d'une table ronde qui s'est tenue le 6 juin dernier et à laquelle a participé Mme Stéphanie Hubert, directrice générale de l'AMAFI.

En suite de cette audition, il a été demandé aux participants de bien vouloir compléter un questionnaire. Le présent document vise à répondre à cette demande.

L'AMAFI représente les acteurs des marchés financiers établis en France. L'Association regroupe plus de 170 institutions françaises et internationales de toutes tailles, notamment des entreprises d'investissement, des établissements de crédit, des courtiers, des bourses et des banques privées. Celles-ci interviennent sur tous les segments de marchés, notamment actions, obligations et dérivés y compris dérivés de matières premières. Par son action, l'Association cherche à promouvoir un cadre réglementaire qui permette le développement de marchés de capitaux robustes, efficaces et compétitifs, au bénéfice des investisseurs, des entreprises et de l'économie en général.

Depuis la publication de la directive et du règlement DORA (*règlement (UE) 2025/2554*), l'AMAFI a été saisie par ses adhérents afin, d'une part, de leur apporter un soutien à l'interprétation de certaines notions[1] et, d'autre part, de les aider à résoudre des difficultés opérationnelles, y compris en organisant des échanges avec l'ACPR[2]. L'Association mène par ailleurs des réflexions sur l'articulation entre l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises des secteurs financiers et DORA, certaines de leurs dispositions traitant des mêmes thématiques (par exemple, l'externalisation).

[1] Par exemple, la question de savoir si un service financier, réglementé ou non, entendu comme un service d'investissement ou un service auxiliaire peut être qualifié de service TIC au sens du règlement DORA. L'intérêt de cette question, désormais tranchée par un document de questions – réponses de la Commission européenne, était de s'assurer qu'une entité financière, déjà soumise à une réglementation sectorielle dense, ne soit pas soumise à des dispositions de DORA qui auraient été inadaptées et redondantes.

[2] Par exemple s'agissant de la déclaration des registres d'informations à l'ACPR (*DORA, art. 28.3*), qui continue de soulever des problèmes importants, pour la résolution desquels l'Association a planifié des réunions avec l'ACPR à la rentrée 2025.

1. Quelles sont les principales menaces liées aux technologies de l'information et de la communication (TIC) auxquelles vous êtes exposées ?

Les principales menaces concernant les entreprises d'investissement sont celles pouvant interrompre la continuité de leurs services, dans un contexte où les marchés nécessitent une présence continue et une capacité de traitement rapide.

Le fonctionnement des marchés financiers repose en outre sur l'interconnexion de leurs participants et des infrastructures de marché, dont certains sont centraux, et qui peuvent faire l'objet d'attaques.

Par ailleurs, la dépendance à certains fournisseurs ou prestataires de nature systémique et/ou jouissant d'une position dominante rend le secteur sensible à des incidents TIC qui se produiraient chez ceux-ci.

Enfin, si la fuite des données personnelles peut être une menace, il est toutefois à noter que les activités de marché de gros que représente l'AMAFI sont essentiellement exercées avec des clients professionnels. La fuite de données, autres que personnelles, est en revanche un point d'attention s'agissant du secret des affaires.

Ainsi, les principales menaces identifiées pour les activités de marché sont les suivantes :

- Attaque par déni de services (DDoS) directement sur une entreprise d'investissement ou indirectement par ricochet (entreprise de marché touchée, affectant plusieurs entreprises d'investissement par exemple)
- Attaques sur les fournisseurs et sous-traitants de manière générale, et en particulier sur ceux avec lesquels une relation de dépendance existe
- Fuites de données

2. Avez-vous des exemples de cyberattaques importantes dont auraient été victimes les entreprises du secteur bancaire ?

Les cyberattaques peuvent être très importantes en nombre, jusqu'à plusieurs milliers par jour par établissement actif dans les activités de marché. Toutefois, nous n'avons pas connaissance de cyberattaques non déjouées dans ce secteur.

3. Est-ce que l'application du règlement européen sur la résilience opérationnelle numérique du secteur financier (*Digital Operational Resilience Act* – DORA) vous pose des difficultés ?

Oui, les principales difficultés identifiées sont exposées ci-après.

- **Relation avec les prestataires**
  - **Difficulté d'application des clauses contractuelles imposées par le règlement DORA.** Les établissements peinent à faire accepter à leurs prestataires les clauses requises, ce qui aboutit à la non-conformité de certains contrats. Par exemple, peu de prestataires tiers

acceptent d'accorder à leurs clients des « *droits illimités d'accès, d'inspection et d'audit* » (*DORA, art. 30.3 e) i)*), tandis que d'autres facturent la participation aux audits. Certains vont même jusqu'à contourner cette obligation en fixant un prix à un niveau dissuasif.

- **Un rapport de force déséquilibré avec les prestataires dominants**. Les acteurs les plus puissants du marché imposent leurs conditions contractuelles, rendant dans les faits quasi impossible la mise en conformité avec les exigences de DORA. Cette difficulté est accentuée par le fait que l'Union européenne est, à ce jour, la seule juridiction à imposer un tel niveau d'exigence.
- **Contraintes opérationnelles fortes pour les audits sur site.** La réalisation d'audits physiques pose d'importantes difficultés pratiques, notamment en ce qui concerne la ségrégation physique des espaces et des environnements informatiques permettant d'individualiser le périmètre des audits. Ces contraintes sont souvent liées à des enjeux de protection des données personnelles, en lien avec le RGPD.

- **Relation avec les autorités**

  - **Manque de coordination entre autorités nationales et européennes.** Les divergences dans l'interprétation et la mise en œuvre des exigences DORA sont notables, par exemple en ce qui concerne les modalités techniques pour les registres d'information qui diffèrent selon les juridictions (quand bien même le modèle de registre a été défini par l'EBA).
  - **Manque de préparation au sein de l'ACPR.** Aucun service dédié n'a été initialement prévu pour le suivi du règlement et la gestion des incidents opérationnels.
  - **Multiplicité des interlocuteurs pour les acteurs transfrontaliers - absence de guichet unique européen.** Chaque État membre disposant de sa propre autorité compétente, les acteurs transfrontaliers doivent composer avec une pluralité d'interlocuteurs, complexifiant les démarches. Par exemple, les modalités de dépôt varient selon les autorités, en l'absence d'un cadre harmonisé à l'échelle européenne, et les entités systémiques ou critiques sont soumises à des dépôts multiples auprès de différentes autorités, sans mécanisme de coordination ni de mutualisation des exigences. Par ailleurs, aucune plateforme centralisée ne permet aux entités, et en particulier celles qui sont présentes dans plusieurs Etats membres de l'UE, de regrouper leurs démarches.

- **Délais de mise en œuvre**

  - **Retard dans la publication des textes de niveau 2.** Les actes délégués et d'exécution ont été publiés tardivement, laissant aux entités un délai de mise en conformité extrêmement court. Certains textes restent encore à paraître, ce qui empêche une planification sereine. (Voir question suivante.)

- **Registre d'informations**
  - **Exigences excessives en matière de chaîne de sous-traitance.** L'obligation d'identifier et de documenter les sous-traitants de second et troisième niveaux soulève des difficultés. Un prestataire tier peut recourir à des centaines de sous-traitants répartis dans de multiples juridictions. Il apparaît disproportionné de faire peser sur les entités financières la responsabilité de collecter et maintenir à jour ces informations, sur lesquelles elles n'ont bien souvent aucun contrôle direct.

- **Exigences techniques**
  - **Format de déclaration des incidents.** Le signalement des incidents majeurs au format .JSON impose aux entités de développer un logiciel dédié en interne ou d'avoir recours à un prestataire. Cette exigence d'un format technique complexe est particulièrement problématique dans un contexte d'urgence, les déclarations devant être transmises dans un délai de 24 heures, souvent en pleine gestion de crise. Certains régulateurs, comme en Irlande, ont opté pour une approche plus pragmatique en mettant à disposition un format simplifié (Excel pour l'Irlande, par exemple), qu'ils convertissent eux-mêmes en fichier .JSON.
  - **Complexité des critères de qualification d'un incident « majeur ».**
  - **Difficulté à respecter le délai de 4 heures pour la déclaration des incidents majeurs** du fait notamment de la fermeture la nuit du système de déclaration de l'ACPR (l'alternative proposée d'utiliser un email pour effectuer la déclaration n'apporte pas les garanties de sécurité nécessaires).

4. Est-ce que les délais d'application vous semblent tenables ?

Le calendrier fixé par le règlement DORA apparaît peu réaliste.

Les normes techniques de niveau 2 ont été publiées très tard, parfois même après l'entrée en application du règlement, le 17 janvier 2025.

Par exemple, les règles détaillant le contenu et les délais de notification des incidents majeurs n'ont été publiées que le 20 février 2025 tandis que les entités devaient s'y conformer dès l'entrée en application du règlement.

De même, l'ITS relatif au modèle de registre d'informations n'a été mis à disposition que début décembre 2024, et les FAQ de l'ACPR ont été mises à jour à plusieurs reprises jusqu'à fin mai 2025, parfois en contradiction avec celles de l'EBA, tandis que la date du premier dépôt avait été fixée au 15 avril 2025.

Ces évolutions tardives, parfois incohérentes, ont rendu impossible une mise en œuvre cohérente, et juridiquement stable des nouvelles obligations. Dans le même temps, les travaux de mise en conformité imposent une charge opérationnelle très importante aux établissements : cartographie exhaustive des prestataires TIC, refonte des processus de notification, mise à jour documentaire, renforcement des dispositifs de contrôle interne, etc. Dans ces conditions, un délai supplémentaire est nécessaire pour garantir une mise en conformité effective et homogène de l'ensemble du secteur.

Au regard de la difficulté de mise en conformité des contrats avec les prestataires tiers, il est probable que la remédiation complète prendra plusieurs années pour l'ensemble de la Place. À titre de comparaison, la mise en conformité des contrats en application du RGPD, en vigueur depuis 2018, n'est toujours pas finalisée pour toutes les entités françaises concernées.

Enfin, la désignation, prévue pour octobre, des prestataires tiers critiques sous supervision européenne aura un impact supplémentaire sur les contrats concernés, complexifiant davantage encore le processus de remédiation.

5. Y a-t-il des difficultés propres aux Outre-mer ? Le président, le rapporteur général et le rapporteur du titre III ont notamment été interpellés par la Fédération bancaire française (FBF) en Nouvelle-Calédonie concernant un problème de délai de mise en œuvre.

L'AMAFI n'est pas en mesure de répondre à cette question, les activités de marché qu'elle représente étant localisées en métropole.

6. Est-ce que l'adaptation aux exigences du règlement DORA représente un coût important pour les entreprises du secteur ?

La mise en œuvre du règlement DORA génère des coûts significatifs pour les entreprises du secteur, tant en matière de ressources humaines que d'investissements techniques. Parmi les principales charges identifiées :

- **Réaffectation des ressources internes**, avec pour conséquence parfois une réduction des effectifs initialement consacrés à la surveillance exclusive des risques cyber, au profit d'activités de mise en conformité DORA ;
- **Développement de solutions logicielles spécifiques** ou **recours à des prestataires externes** ;
- **Mise en place d'une politique de formation interne**, visant à sensibiliser et à former les équipes aux nouvelles obligations réglementaires et aux processus associés ;
- **Remédiation contractuelle**, qui implique un travail juridique et opérationnel de grande ampleur, avec des coûts non négligeables liés à la revue, à la renégociation et à la mise à jour des contrats avec les prestataires tiers, nécessitant souvent le recours à des conseils juridiques coûteux ;
- **Allocation de nouvelles ressources dédiées à la conformité DORA**, se traduisant par une hausse des charges de personnel et une pression accrue sur les fonctions de conformité et de gestion des risques ;
- **Charges supplémentaires imposées par les prestataires TIC,** notamment pour la conduite d'audit, voire renégociation des tarifications à la hausse à l'occasion de la revue des contrats.

7. Quel est votre avis sur ces modifications apportées au titre III du projet de loi (résilience opérationnelle numérique du secteur financier) par le Sénat en première lecture :

a) Sur la désignation d'une seule autorité compétente pour la déclaration des incidents majeurs liés aux TIC et la notification volontaire des cybermenaces importantes (articles 43 A et 45 *bis*) ?

La désignation d'une autorité unique compétente pour centraliser les déclarations d'incidents majeurs liés aux TIC et les notifications volontaires de cybermenaces importantes constitue une avancée bienvenue. Une telle centralisation est de nature à simplifier les obligations déclaratives des entités financières tout en assurant une coordination plus efficace des réponses en cas d'incident.

La question du choix de cette autorité mérite cependant une attention particulière. L'AMAFI considère que certains éléments militent pour l'attribution de cette compétence à l'ANSSI. En effet, celle-ci dispose de l'expertise et des capacités opérationnelles nécessaires pour accompagner les entités concernées face à des situations critiques, notamment via le dispositif CERT-FR.

Ni l'ACPR ni la Banque de France ne disposent, à ce jour, d'une structure équivalente dédiée au traitement technique et à la réponse aux incidents TIC de grande ampleur. L'ACPR ne dispose pas d'un service accessible en continu pour la réception de ces notifications. Par ailleurs, le recours à l'envoi par courriel en cas d'indisponibilité du portail OneGate n'est pas satisfaisant, notamment au regard des exigences de sécurité et de confidentialité inhérentes à ce type de communication.

En outre, des dysfonctionnements ont été signalés concernant le portail OneGate lui-même, notamment en ce qui concerne la gestion des droits d'accès, avec des cas de failles dans l'attribution de ces droits. Ces constats soulignent la nécessité d'un dispositif technique plus robuste et sécurisé pour assurer un traitement fiable des notifications d'incidents.

Dès lors, confier cette mission à l'ANSSI pourrait permettre de renforcer la sécurité et l'efficacité du dispositif tout en assurant une cohérence avec les obligations introduites par la directive NIS 2, celle-ci désignant également l'ANSSI comme autorité de référence en matière de cybersécurité pour les signalements d'incidents majeurs dans le secteur financier.

b) Sur l'extension de l'application du règlement DORA aux succursales d'entreprises d'investissement de pays hors UE (article 49 bis) ?

Il s'agit ici d'appliquer les exigences de DORA aux succursales en France d'établissements de pays tiers (hors UE).

Si cette volonté est cohérente avec l'approche historiquement adoptée par la France à l'égard de ces succursales et assure une égalité du champ concurrentiel entre acteurs établis dans le pays, elle pourrait toutefois venir amoindrir l'attractivité de la France si les autres États de l'UE ne mettaient pas en place de mesures nationales analogues. Pour garantir l'harmonisation européenne, il conviendrait donc de que la France porte cette exigence au niveau européen.

c) Sur l'inversion de la charge de la preuve vis-à-vis des assurances en cas de cyberattaque (article 58 *bis*) ?

L'AMAFI n'a pas d'observation sur cet aspect.

d) Sur le fait d'empêcher un assujettissement à la directive NIS 2 des entités financières déjà soumises à la directive et au règlement DORA (article 62 A) ?

Ceci est une très bonne initiative, dans la mesure ou les exigences de NIS2 sont toutes couvertes par DORA, qui est une régulation sectorielle dédiée au secteur financier, ceci avec souvent un niveau d'exigence plus élevé.

Pour autant, il conviendrait que cette disposition ne soit pas limitée aux entités financières essentielles et importantes. Toutes les entités financières dans le champ de DORA devraient pouvoir être exemptées.

Par ailleurs, cette exemption devrait pouvoir être applicable au niveau européen : certaines succursales établies dans l'UE pourraient être soumises à NIS2 localement alors même que leur entité mère établie en France ne le serait pas. Il conviendrait donc de porter cette exemption au niveau européen à l'occasion d'une modification de DORA.

e) Sur le report de l'entrée en vigueur de plusieurs mesures pour les sociétés de financement (article 62) ?

L'AMAFI ne représente pas les sociétés de financement.

8. Plus largement, quelles informations souhaitez-vous porter à la connaissance du rapporteur concernant le titre III du projet de loi, la directive ou le règlement DORA ?

Une approche conduisant à une charge administrative disproportionnée

L'AMAFI relève que, bien que le principe de proportionnalité soit mentionné dans le règlement DORA, sa mise en œuvre demeure purement théorique.

En effet, les critères définis sont formulés en des termes trop généraux pour permettre une application concrète et différenciée. En pratique, aucune entité, quelle que soit sa taille ou la nature de ses activités, ne semble en mesure de bénéficier effectivement d'un allègement des exigences sur cette base. Par exemple, les établissements non essentiels et importants devraient pouvoir bénéficier d'allègements.

Plus généralement, alors que la Commission a dévoilé ses objectifs de simplification réglementaire et de réduction de la charge pesant sur les entreprises, DORA est révélateur d'une logique administrative particulièrement lourde en matière règlementaire.

L'objectif de meilleure maitrise du risque cyber, notamment par l'identification par les acteurs financiers de leurs domaines de vulnérabilité, a abouti à exiger d'eux une masse d'informations très

conséquente. Le souci de couverture totale a pris le pas sur une approche ciblée et proportionnée : la capacité des établissements à apprécier eux-mêmes la gravité et la criticité de leurs risques a été remplacée par une logique déclarative standardisée, à la fois lourde et parfois peu pertinente.

Par ailleurs, l'exigence de résultat induite par DORA et pesant sur les établissements se heurte en pratique, comme évoqué à la question 3, à la résistance de certains prestataires TIC dominants, ou pour les acteurs financiers de plus petite taille, à des rapports de force commerciaux très déséquilibrés. Dans ce contexte, il serait pragmatique que DORA intègre des dispositions reconnaissant la notion de "meilleurs efforts" en matière de mise en conformité. Une telle approche permettrait aux entités concernées de démontrer la réalité de leur engagement, sans encourir de sanctions dans des situations où les obstacles sont structurellement indépendants de leur volonté.

Les objectifs peu compatibles de DORA et FIDA

L'AMAFI attire l'attention sur une incohérence structurelle entre le règlement DORA et le règlement FIDA. Le premier impose un renforcement des exigences de sécurisation des systèmes d'information, tandis que le second prévoit une ouverture plus large des données financières, au-delà de ce que permet la directive DSP2, sur la base du consentement du client.

Cette situation crée une tension entre deux logiques difficilement conciliables : d'un côté, un encadrement plus strict des systèmes pour limiter les risques cyber, et de l'autre, une facilitation de l'accès aux données par des tiers, potentiellement moins robustes ou plus exposés sur le plan de la cybersécurité. Cette contradiction pourrait compromettre la cohérence globale du dispositif de cybersécurité du secteur financier.

L'AMAFI estime qu'un tel déséquilibre soulève des risques opérationnels concrets. En cas de fuite de données, l'identification de la source deviendrait sensiblement plus complexe, rendant plus difficile la gestion des incidents et la mise en œuvre de mesures correctives. Il apparaît donc essentiel que cette problématique soit prise en compte dans les travaux parlementaires, afin de garantir une articulation cohérente des textes européens en matière de sécurité et d'ouverture des données.