FSMA
AUTORITÉ DES SERVICES ET MARCHÉS FINANCIERS

Communication

FSMA_2025_01 du 17-01-25

Une deuxième enquête réalisée par la FSMA montre que les entités financières doivent encore fournir des efforts pour se conformer au règlement DORA

Champ d'application:

Les entités financières qui sont soumises au règlement européen DORA

Résumé/Objectifs:

L'Autorité des services et marchés financiers (FSMA) a réalisé en novembre 2024 une deuxième enquête visant à vérifier le degré de préparation des entités financières à l'entrée en application du règlement européen DORA, prévue le 17 janvier 2025. Les résultats de cette deuxième enquête montrent que de nombreuses entités financières sont sur la bonne voie pour satisfaire aux objectifs fixés par le règlement DORA, mais qu'elles devront encore fournir des efforts importants pour se conformer entièrement à ses dispositions.

L'Autorité des services et marchés financiers (FSMA) a réalisé en novembre 2024 une deuxième enquête visant à vérifier le degré de préparation des entités financières à l'entrée en application du règlement européen DORA (« *Digital Operational Resilience Act* »), prévue le 17 janvier 2025. Le règlement DORA fixe des objectifs ambitieux en matière de résilience opérationnelle numérique, dont la finalité est de protéger les entités financières et leurs clients. Les résultats de cette deuxième enquête montrent que de nombreuses entités financières sont sur la bonne voie pour satisfaire aux objectifs fixés par le règlement DORA, mais qu'elles devront encore fournir des efforts importants pour se conformer entièrement à ses dispositions. Compte tenu de l'entrée en application imminente du règlement, ces entités ont encore un défi important à relever. En raison du faible taux de participation à l'enquête, le niveau de mise en œuvre du règlement DORA reste par ailleurs difficile à cerner auprès d'une proportion non négligeable d'entités soumises aux exigences de ce règlement.

Après une première enquête menée fin 2023, la FSMA a lancé en octobre 2024 une deuxième enquête plus étoffée dans le but d'évaluer le niveau de mise en œuvre, auprès des entités financières, des différentes exigences prévues par le règlement DORA. La FSMA voyait également dans cette enquête l'opportunité de procurer aux entités financières un outil pratique leur permettant d'effectuer une *gap analysis* entre les exigences DORA et leur état d'implémentation actuel. Cette enquête pouvait ainsi leur servir de fil conducteur pour identifier les exigences - sur le plan de la gestion du risque lié aux TIC, de la gestion des incidents, des tests de résilience numérique et de la gestion de prestataires tiers de services TIC - qu'elles devaient encore organiser, développer et mettre en œuvre avant l'entrée en application du règlement DORA le 17 janvier 2025.

Cette enquête non contraignante de la FSMA, qui reposait sur une autoévaluation des entités, a été lancée le 21 octobre 2024 et clôturée 6 semaines plus tard, soit le 29 novembre 2024. Au final, 93 des entités visées y ont répondu, ce qui représente un taux de participation global de 36 %. Il est préoccupant de constater que ce taux de participation global est inférieur de 14 points de pourcentage à celui observé lors de la première enquête organisée par la FSMA en 2023. Cela pourrait indiquer que les préparatifs à l'entrée en application du règlement DORA ne se déroulent pas de manière optimale auprès de nombreuses entités financières. Si tel est le cas, ces dernières sont instamment invitées à entreprendre les démarches nécessaires pour se conformer aux dispositions du règlement qui leur sont applicables.

Le taux de participation a globalement diminué par rapport à la première enquête

L'analyse du taux de participation montre que 60 % des OPCVM autogérés et 50 % des prestataires de services de financement participatif (*crowdfunding*) ont répondu à l'enquête, alors qu'ils en avaient été les grands absents en 2023. La FSMA s'en réjouit, tout comme elle salue le taux de participation plus élevé du côté des intermédiaires d'assurance (y compris ceux à titre accessoire) et des intermédiaires de réassurance (28 % contre 19 % lors de la première enquête). La FSMA se réjouit également de constater le maintien d'un taux de participation élevé parmi les sociétés de gestion de portefeuille et de conseil en investissement (88 % contre 94 % lors de la première enquête) et les gestionnaires d'OPC(A) (81 % contre 88 % lors de la première enquête).

Malgré ces tendances positives, le taux de participation des intermédiaires d'assurance (y compris ceux à titre accessoire) et des intermédiaires de réassurance reste notablement bas. La baisse significative du taux de participation des institutions de retraite professionnelle (25 % contre 57 % lors de la première enquête) est également frappante.

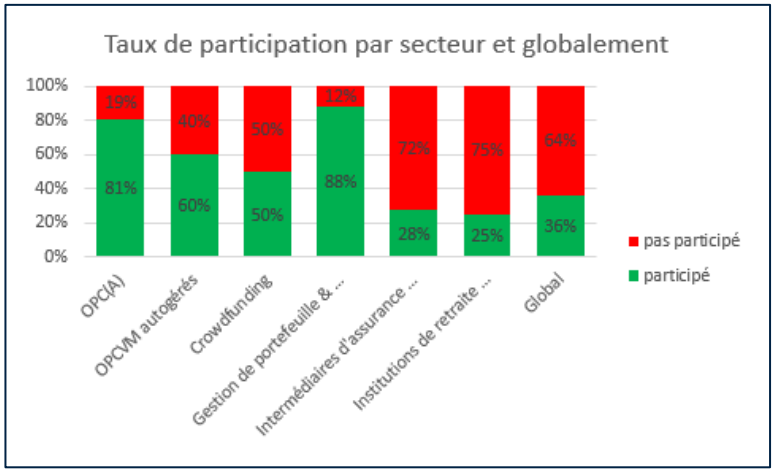

Figure 1 : Taux de participation par secteur et globalement

Une analyse plus approfondie montre que 62 % des entités ayant répondu à la deuxième enquête avaient également participé à la première. La proportion de ces entités dans les secteurs Gestion de portefeuille & Conseil en investissement et OPCA est restée pratiquement la même, mais elle a radicalement changé dans les autres secteurs par rapport à la première enquête.

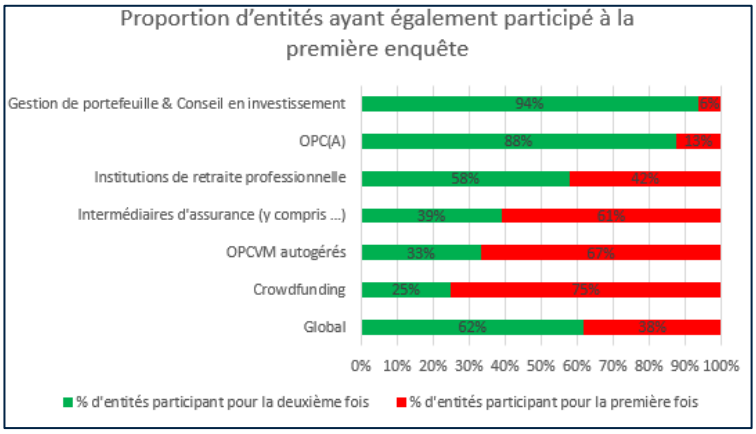

Figure 2 : Proportion d'entités ayant participé aux deux enquêtes ou non

Compte tenu de ces différences observées entre les deux enquêtes au niveau de la population, tant en termes de taille que de type de participants, il n'a pas été aisé pour la FSMA d'établir des comparaisons correctes dans son analyse des résultats. Toute comparaison opérée doit dès lors être considérée en gardant à l'esprit ces différences de population.

Le niveau de maturité tel qu'estimé par les entités participantes pour chaque thème DORA progresse globalement, sauf sur le plan de la gestion des risques liés aux prestataires tiers de services TIC.

Comme dans la première enquête, les entités financières ont été invitées à évaluer, sur une échelle de 1 (faible) à 5 (très élevé), leur « niveau de maturité » par rapport aux quatre grands thèmes DORA explorés dans cette enquête. Dans l'ensemble, le niveau de maturité semble augmenter dans une mesure plus (*gestion du risque lié aux TIC*) ou moins (*gestion, classification et notification des incidents liés aux TIC* et *tests de résilience opérationnelle numérique*) grande. Toutefois, le thème de la *gestion des risques liés aux prestataires tiers de services TIC* constitue une exception, car on observe ici une baisse du niveau de maturité. Il n'a pas été possible d'en déterminer la raison. Il est possible que cette évolution soit due à la différence de population, évoquée plus haut, entre la première et la deuxième enquête.

La figure 3 montre les tendances de manière globale et par secteur.

	Gestion du risque lié aux TIC		Gestion, classification et notification des incidents liés aux TIC		Tests de résilience opérationnelle numérique		Gestion des risques liés aux prestataires tiers de services TIC	
	2023	2024	2023	2024	2023	2024	2023	2024
OPC(A)	3,09	3,24	3,18	3,24	2,25	2,35	2,9	2,82
Gestion de portefeuille & Conseil en investissement	2,56	4	2,13	2,53	1,9	2,6	2,94	2,93
Plateformes de crowdfunding	NA	2,75	NA	2,25	NA	2,25	NA	1,75
Institutions de retraite professionnelle	2,42	2,27	2,26	2,2	2,2	2,07	2,72	2,13
Intermédiaires d'assurance et de réassurance	3,86	3,35	3,79	3,3	2,5	3,19	3,23	2,7
OPCVM autogérés	NA	3	NA	3	NA	3	NA	3
Global	2,67	2,87	2,49	2,74	2,38	2,5	2,766	2,53

Figure 3 : Niveau de maturité moyen de manière globale et par secteur, tel qu'indiqué par les entités participantes (comparaison entre 2023 et 2024)

Bien que le taux de participation soit plus faible, les progrès accomplis par les entités participantes sont plutôt encourageants. Elles doivent néanmoins poursuivre leurs efforts sans relâche afin d'être prêtes pour la mise en œuvre des règles DORA.

Comme lors de la première enquête, les réponses fournies à cette deuxième enquête procédaient d'une autoévaluation. Les entités concernées ne devaient pas étayer leurs affirmations par des explications détaillées, ni par des documents. L'enquête, à laquelle la participation était volontaire, était divisée en quatre parties, correspondant chacune à une section du règlement DORA. Par rapport à la première enquête, les questions ont été posées à un niveau beaucoup plus détaillé. Cette enquête plus étoffée a permis à la FSMA et aux entités participantes d'examiner et d'évaluer la mise en œuvre de chaque article du règlement DORA.

La plupart des entités financières déclarent disposer d'un cadre de gestion du risque lié aux TIC et, notamment, d'une politique de continuité en la matière

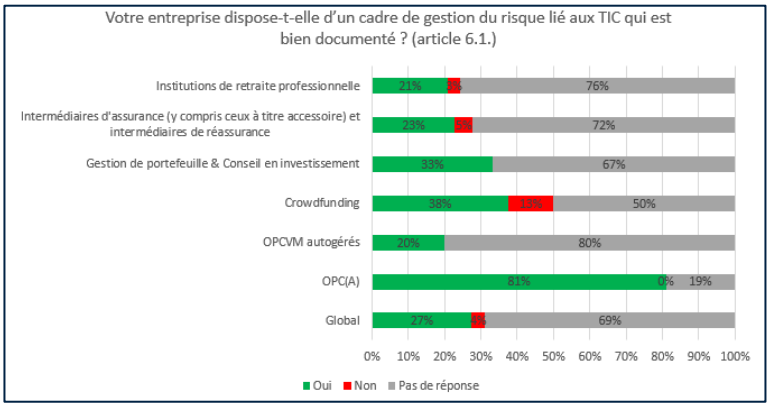

Figure 4 : Proportion d'entités disposant d'un cadre de gestion du risque lié aux TIC qui est bien documenté

Dans chaque secteur, la grande majorité des entités participantes ne relevant pas du régime simplifié ont indiqué qu'elles disposaient d'un **cadre de gestion du risque lié aux TIC** qui est bien documenté.

Par rapport à l'enquête de 2023, le pourcentage d'entités déclarant disposer d'un tel cadre a également augmenté de manière significative.

Grâce aux questions plus détaillées de cette deuxième enquête, la FSMA a également pu vérifier si ce cadre documenté contenait tous les éléments énoncés à l'article 6.2 du règlement DORA. Les résultats montrent que cet aspect est moins satisfaisant. Ainsi, environ 1 entité sur 3 a indiqué que ce cadre ne contenait pas tous les éléments. Même s'il n'est pas encourageant, ce constat est positif dans la mesure où il montre que ces entités ont procédé à une évaluation et savent donc quels sont les points qui nécessitent une attention supplémentaire.

Tous secteurs confondus, plus de 90 % des entités ayant participé à l'enquête ont affirmé disposer d'une **politique de continuité des activités de TIC**, qui est également applicable aux fonctions critiques liées aux TIC qui sont sous-traitées. Bien qu'une légère amélioration puisse être observée par rapport à la première enquête, celle-ci n'est pas très significative. Néanmoins, le pourcentage de réponses positives reste également encourageant dans cette deuxième enquête.

Ce qui est moins encourageant, c'est qu'environ 40 % des entités participantes ont indiqué que ce plan de continuité des activités de TIC ne répondait pas aux objectifs énoncés à l'article 11.2 du règlement. Cet article prévoit notamment que la politique de continuité des activités de TIC doit être mise en œuvre au moyen de dispositifs, de plans, de procédures et de mécanismes spécifiques, appropriés et documentés visant, entre autres, à garantir la continuité des fonctions critiques ou importantes, à répondre aux incidents liés aux TIC et à résoudre ceux-ci rapidement, dûment et efficacement de manière à limiter les dommages. Le fait que seule une petite majorité d'entités indique être en conformité avec cette disposition laisse entendre que de nombreuses entités devront encore fournir des efforts pour que leur politique de continuité des activités en place et documentée soit plus performante et conforme aux exigences du règlement DORA.

Les entités financières doivent améliorer leur capacité de réaction face à des incidents liés aux TIC

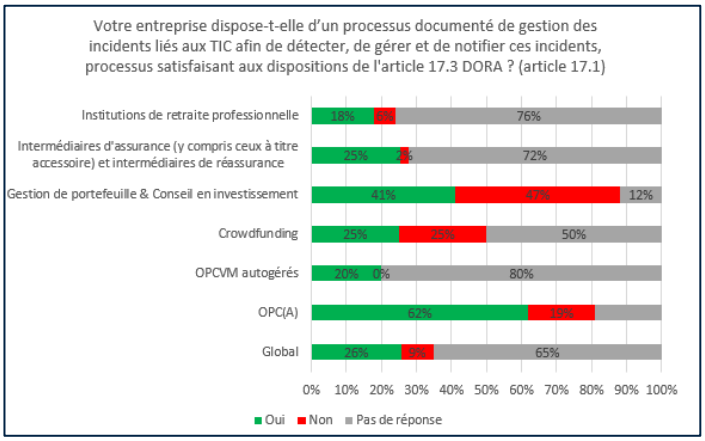

Figure 5 : Processus de gestion des incidents liés aux TIC

Si la plupart des entités financières disposent d'un cadre de gestion du risque lié aux TIC, elles sont moins nombreuses à indiquer qu'elles sont également en mesure de détecter, de gérer et, le cas échéant, de notifier tout incident lié aux TIC. Les résultats de cette deuxième enquête sont très similaires à ceux de la première enquête, en ce sens que peu d'évolution positive est observée.

La FSMA tient donc une nouvelle fois à souligner que cette capacité de réaction et la gestion des incidents liés aux TIC font partie intégrante de la résilience opérationnelle des entités financières face aux cybermenaces. Afin de réduire l'impact de ces incidents, ainsi que les coûts qu'ils engendrent, et d'empêcher leur propagation aux clients et à d'autres entités financières, il est primordial que les entités continuent à améliorer leur capacité de réaction dans ce domaine.

La définition de cadres de gestion du risque et de politiques en matière de TIC n'est rien sans leur mise à l'épreuve

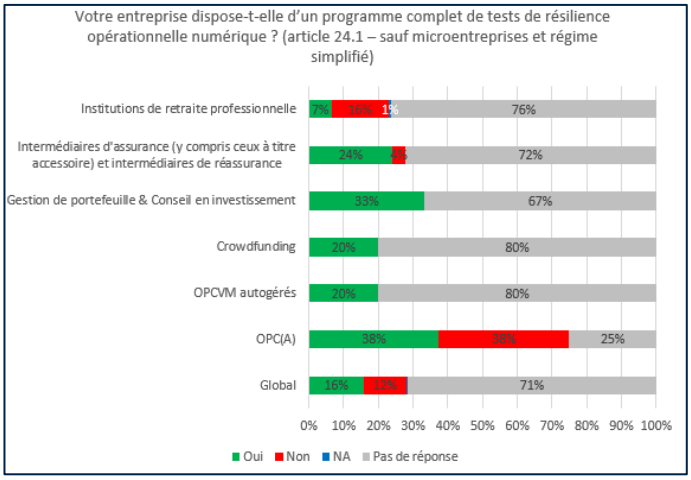

Figure 6 : Proportion d'entités disposant d'un programme de tests de résilience opérationnelle numérique

Ni la mise en place d'un cadre de gestion du risque lié aux TIC, ni la définition de politiques et de procédures en la matière ne sauraient garantir à elles seules la résilience opérationnelle numérique d'une entité financière. La mise au jour des vulnérabilités et du risque lié aux TIC est fondamentale pour s'assurer de l'effectivité et de l'efficacité des mesures mises en place.

Or, une proportion importante des entités participantes (environ 43 %) ne disposent pas encore d'un programme complet de tests de résilience opérationnelle numérique. Il s'agit d'une amélioration par rapport à l'enquête précédente, mais ce pourcentage reste particulièrement faible. A noter que les microentreprises et les entités relevant du cadre simplifié ont été volontairement omises du calcul, les premières devant mettre en place un programme de tests proportionnel et les secondes ne devant pas posséder un tel programme.

Il est également frappant de constater que, dans certains secteurs, toutes les entités participantes ont indiqué qu'elles disposaient d'un tel programme de tests. Tant dans le secteur Gestion de portefeuille & Conseil en investissement que du côté des OPCVM autogérés et des Plateformes de *crowdfunding*, l'ensemble des entités semblent avoir mis en place ce programme de tests. Il convient toutefois de nuancer ce constat car la quasi-totalité des entités du secteur Gestion de portefeuille & Conseil en investissement n'ont pas été incluses dans le graphique ci-dessus, étant donné qu'elles relèvent du cadre simplifié de gestion du risque lié aux TIC, et le nombre absolu d'entités des deux autres secteurs est très faible.

Il est par contre tout à fait remarquable que la grande majorité (84 %) des intermédiaires d'assurance (y compris ceux à titre accessoire) et des intermédiaires de réassurance ayant participé à l'enquête

aient indiqué qu'ils disposaient également d'un tel plan. Il convient toutefois de rappeler que le taux de participation de ce dernier secteur est très faible.

La FSMA a également vérifié quel pourcentage des entités participantes effectuaient tels ou tels tests. Le résultat de cette analyse figure dans le tableau ci-après. Il est à nouveau frappant d'observer que la grande majorité des intermédiaires d'assurance (y compris ceux à titre accessoire) et des intermédiaires de réassurance ayant répondu à l'enquête ont indiqué qu'ils effectuaient presque tous les tests.

Secteur	1.vulnera-bility_scan	2.open_source _analyses	3.source_ code	4.network _security	5.gap_ana -lyses	6.physical _security	7.detec-tion tools	8.scenario	9.compa-tibility	10.perfor-mance	11.end-to-end	12.pene-tration	13.TLPT
OPC(A)	35%	18%	12%	29%	29%	35%	35%	24%	18%	12%	18%	29%	6%
Crowdfunding	25%	25%	25%	0%	0%	0%	0%	25%	0%	25%	0%	25%	0%
Institutions de retraite professionnelle	23%	19%	23%	26%	16%	16%	19%	19%	23%	23%	19%	19%	3%
Gestion de portefeuille & Conseil en investissement	40%	13%	7%	40%	33%	27%	40%	7%	20%	13%	7%	40%	13%
Intermédiaires d'assurance (y compris ceux à titre accessoire) et intermédiaires de réassurance	87%	48%	78%	78%	70%	83%	74%	74%	70%	78%	70%	78%	43%
OPCVM autogérés	100%	0%	0%	0%	100%	0%	0%	0%	0%	0%	0%	100%	0%
Global	45%	25%	32%	41%	35%	37%	38%	32%	32%	33%	29%	41%	15%

Figure 7 : Proportion d'entités effectuant des tests spécifiques

Les entités doivent améliorer la gestion des risques liés aux prestataires tiers de services TIC

97 % des entités ayant participé à l'enquête ont déclaré faire appel à des prestataires tiers de services TIC. Toutefois, 43 % d'entre elles déclarent ne pas disposer d'une stratégie pour gérer les risques liés à ces prestataires. Un peu moins de la moitié des entités sans stratégie (42 %) précisent certes à juste titre que la mise en place d'une telle stratégie ne fait pas partie des exigences que leur impose le règlement.

Cela signifie tout de même qu'environ 1 entité participante sur 3 soumise à cette disposition du règlement indique qu'elle n'a pas élaboré de stratégie de gestion des risques liés aux prestataires tiers, alors qu'il s'agit d'une exigence à remplir. L'entité restant en toute hypothèse pleinement responsable du respect du règlement, il est essentiel qu'elle élabore également une stratégie sous-tendant la gestion de ces risques. Il est donc vivement conseillé aux entités n'ayant pas encore satisfait à cette exigence de faire le nécessaire pour s'y confirmer rapidement.

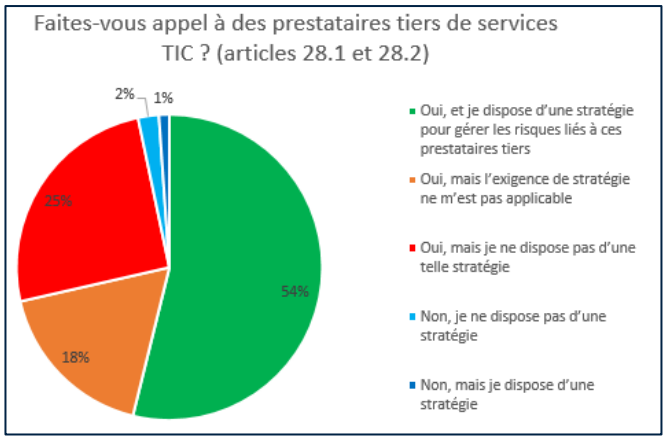

Figure 8 : Proportion d'entités faisant appel à des prestataires tiers et disposant d'une stratégie ou non

Aujourd'hui, DORA est vraiment là !

Les résultats présentés ci-dessus montrent que de nombreuses entités ayant participé à cette enquête devront encore prendre des mesures importantes pour se conformer aux exigences du règlement DORA.

Il est en outre regrettable de constater que les entités financières ont été moins nombreuses à répondre à cette enquête qu'à la première. La proportion d'entités participantes est par ailleurs faible, voire très faible pour certains secteurs. La FSMA n'est ainsi pas en mesure d'avoir une vue précise du degré de mise en œuvre des dispositions du règlement parmi les entités qui n'ont pas participé à l'enquête.

La FSMA espère néanmoins que toutes les entités financières concernées auront profité de la période séparant la conclusion de cette enquête et l'entrée en application du règlement pour se préparer à ce cap de manière adéquate et suffisante.

La FSMA s'appuiera notamment sur ces premières constatations pour orienter ses futures actions de contrôle. Elle pourra à l'avenir mener d'autres enquêtes auxquelles les entités seront obligées de participer et, dans ce cadre, demander à ces dernières d'étayer ou de prouver leurs réponses à l'aide de documents supplémentaires. Cette façon d'opérer permettra à la FSMA d'approfondir son évaluation de la conformité des entités aux exigences du règlement DORA. Ces initiatives viseront également à mesurer et à renforcer en permanence la résilience opérationnelle numérique des acteurs du secteur financier.

Tout en tenant compte des limites de cette enquête et des observations qui peuvent en être tirées, la FSMA appelle les entités financières à considérer la mise en œuvre des règles DORA comme une priorité en 2025, en mettant l'accent sur les aspects suivants :

- accroître continuellement la maturité de la gestion des risques et, plus spécifiquement, mettre en place un plan de continuité des activités conforme à l'article 11.2 du règlement DORA,
- développer une gestion adéquate et efficace des incidents liés aux TIC,
- être en mesure d'évaluer et de gérer les risques liés au recours fait à des prestataires tiers de services TIC.