N°4160
Entrée le 06.07.2026
Chambre des Députés

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère des Finances

Réponse du ministre des Finances, Gilles Roth, à la question parlementaire n° 4160 du 1er juin 2026 de l'honorable député Sven Clement concernant le bilan des notifications DORA à la CSSF

1. **Combien de notifications d'incidents ICT majeurs la CSSF a-t-elle reçues depuis le 17 janvier 2025 ? Le Ministre peut-il fournir une ventilation par type d'entité financière (établissements de crédit, entreprises d'investissement, sociétés de gestion, PSF, prestataires de services de paiement, etc.) ?**

Selon les données transmises par la CSSF, 326 notifications d'incidents ICT majeurs ont été reçues entre le 17 janvier 2025 et le 8 juin 2026.

La répartition par type d'entités est la suivante : 40% proviennent des établissements de crédit, 19% des gestionnaires de fonds d'investissement et 10% des PSF spécialisés. Les 31% restants concernent d'autres entités surveillées, notamment les entreprises d'investissement, les établissements de paiement, les PSF de support et les établissements de monnaie électronique.

2. **Combien de notifications de cybermenaces significatives ont été reçues sur cette même période ?**

1 notification volontaire de cybermenace significative a été reçue par la CSSF.

3. **Quelles sont les principales typologies d'incidents notifiés (ransomware, compromission de données, défaillance de prestataire ICT tiers, déni de service, défaillance applicative) et quelles tendances se dégagent par rapport aux notifications reçues sous l'ancien régime de la circulaire CSSF 24/847 ?**

Les incidents notifiés sont liés à des défaillances de prestataires tiers (29,5 %), des défaillances techniques (26,3 %), des défaillances de processus (21,1 %) et erreurs humaines (10,69 %), et des actions malveillantes (12,4 %).

La CSSF note une augmentation du volume global de notifications, qui s'explique principalement par l'élargissement du périmètre des entités financières assujetties et par une sensibilisation accrue des acteurs du marché au nouveau cadre européen DORA. La typologie des incidents notifiés reste toutefois globalement inchangée.

4. **Quel est le délai moyen constaté entre la survenance d'un incident et la soumission de la notification initiale par l'entité financière ? Dans combien de cas le délai réglementaire de 4 heures pour la notification initiale et de 72 heures pour le rapport intermédiaire n'a-t-il pas été respecté ?**
5. **Dans combien de cas la CSSF a-t-elle jugé une notification incomplète et demandé un complément d'information ? Quel est le délai moyen de soumission du rapport final clôturant un incident ?**
6. **Combien d'entités financières avaient effectivement créé le rôle eDesk « IT Incident Notifier » au 17 janvier 2025 et combien ne l'avaient pas encore fait, compromettant ainsi leur capacité à notifier dans les délais ?**

Réponse aux questions 4 à 6

Il convient de préciser que la notification initiale doit être transmise dans les 4 heures suivant la classification par l'entité de l'incident comme incident ICT majeur, et au plus tard dans les 24 heures après que l'entité a pris connaissance de l'incident.

Les échéances applicables sont respectées dans la très grande majorité des cas. Lorsque des retards ou difficultés opérationnelles sont constatés dans le processus de notification, la CSSF assure un suivi afin d'identifier les causes et de veiller à la mise en place de mesures appropriées visant à renforcer les dispositifs de gestion et de *reporting* des incidents.

Le délai moyen de soumission du rapport final est d'environ 26 jours après la notification initiale.

En janvier 2025, 54 % des entités relevant du champ d'application de DORA avaient mis en place le rôle eDesk « IT Incident Notifier ». Ce taux s'élève aujourd'hui à 85 %.

L'absence de création de cet accès préalablement à la survenance d'un incident n'implique pas nécessairement un retard dans la notification. Le cas échéant, l'entité concernée peut également prendre contact directement avec la CSSF par d'autres moyens.

7. **La CSSF a-t-elle identifié des cas où un incident ICT majeur aurait dû être notifié mais ne l'a pas été ? Quels mécanismes de détection des sous-notifications la CSSF a-t-elle mis en place ?**
8. **La CSSF a-t-elle procédé à des contrôles proactifs, des exercices de simulation ou des inspections sur place pour vérifier la capacité des entités financières à classifier correctement un incident et à le notifier dans les délais requis ?**
9. **Combien de mesures de supervision ou de sanctions la CSSF a-t-elle prises à l'encontre d'entités financières pour défaut, retard ou insuffisance de notification d'incident ICT majeur depuis le 17 janvier 2025 ? Si aucune mesure n'a été prise, comment le Ministre explique-t-il l'absence de recours à cet outil, alors que DORA prévoit des amendes pouvant atteindre 10 millions d'euros ou 2% du chiffre d'affaires mondial ?**

Réponse aux questions 7 à 9

La CSSF n'a pas connaissance d'un cas où un incident ICT majeur aurait dû être notifié mais ne l'aurait pas été.

Aucune procédure de sanction administrative n'a été actée à l'encontre d'une entité pour défaut, retard ou insuffisance de notification d'un incident ICT majeur.

Les dispositifs de gestion et de notification des incidents ICT font partie du périmètre des activités de surveillance de la CSSF. Ils peuvent notamment être examinés dans le cadre de contrôles sur place portant sur la gestion des risques ICT, ainsi que lors de l'analyse des *reportings* annuels transmis par les entités.

10. **La CSSF a annoncé en février 2025 le report de l'obligation de notification les week-ends et jours fériés pour certaines entités, en raison de la non-transposition de la directive NIS2 au Luxembourg. Ce report est-il toujours en vigueur ? Le Ministre peut-il préciser combien d'entités sont concernées et quand cette obligation sera effective ? Des incidents survenus un week-end ou un jour férié ont-ils, de ce fait, été notifiés avec un retard significatif ?**

Le report temporaire des obligations de notification les week-ends et jours fériés pour certaines entités est resté actif jusqu'à l'entrée en vigueur de la loi NIS 2 au Luxembourg, date à laquelle il a pris fin.

Au total, 164 entités sont concernées par cette obligation , dont 123 banques et 41 PSF de support.

A ce jour et depuis l'entrée en application de cette obligation, la CSSF n'a pas connaissance de la survenance d'incidents durant le week-end ou un jour férié qui aurait dû déclencher une notification.

11. **Combien d'entités financières ont soumis leur registre d'informations (Register of Information) dans les délais impartis en avril 2025 ? Combien de registres ont été rejetés par la CSSF ou les autorités européennes de supervision (ESAs) pour erreurs ou incomplétude ?**

387 des 389 entités financières devant soumettre leur registre d'informations à la CSSF ont communiqué une version acceptée par la CSSF dans les délais impartis. Ces registres ont été transmis aux autorités européennes de supervision, dont 357 ont été acceptés à ce jour.

12. **Parmi les incidents ICT majeurs notifiés, quelle proportion impliquait un prestataire ICT tiers ? La CSSF dispose-t-elle d'une vue consolidée des prestataires tiers les plus fréquemment impliqués dans des incidents affectant la place financière luxembourgeoise ?**

La CSSF dispose d'une vue consolidée des prestataires tiers les plus fréquemment impliqués dans des incidents affectant la place financière luxembourgeoise.

Un quart des incidents ICT majeurs notifiés à la CSSF impliquent un prestataire ICT tiers.

13. **Comment la coordination entre la CSSF, le HCPN, le CIRCL et, le cas échéant, la BCE s'organise-telle concrètement lors de la réception d'une notification d'incident ayant un impact transfrontalier ou affectant une entité sous supervision directe de la BCE ?**

14. **La CSSF prévoit-elle de publier des statistiques agrégées ou un rapport sur les incidents ICT majeurs notifiés, afin de renforcer la transparence et de permettre au secteur d'en tirer des enseignements collectifs ?**

<u>Réponses aux questions 13 et 14</u>

La CSSF a mis en place un mécanisme de transmission des notifications à toutes parties prenantes selon les compétences respectives (notamment la BCL, le HCPN, le CIRCL et/ou le GOV-CERT (CSIRT du Luxembourg)) et en ligne avec le cadre légal applicable. Les notifications d'incidents majeurs des entités soumises à la supervision directe de la BCE sont transmises automatiquement à celle-ci.

Conformément au cadre européen DORA, les incidents ICT majeurs notifiés aux autorités nationales font l'objet d'une consolidation au niveau européen. Les autorités européennes de surveillance publient, sur cette base, des analyses consolidées permettant d'identifier les principales tendances, de renforcer la transparence et de partager les enseignements utiles avec le secteur financier.

15. **Combien d'agents de la CSSF sont actuellement affectés au traitement et à l'analyse des notifications d'incidents ICT sous DORA et du contrôle onside des TICs? Le Ministre estime-t-il que ces moyens sont suffisants au regard du volume attendu de notifications, sachant que le périmètre DORA couvre plus de 20 types d'entités financières ?**

Au sein de la CSSF, une équipe horizontale de 20 agents est spécialisée dans la surveillance « off-site » des risques TIC des entités, y compris le traitement et l'analyse des notifications d'incidents ICT. S'y ajoute une équipe d'agents affectés aux activités d'audit et de contrôle sur place (surveillance « on-site ») dans le domaine des TIC. En sus de ces équipes spécialisées « off-site » et « on-site », tous les services de surveillance en charge de la surveillance globale des entités jouent également un rôle croissant dans la surveillance de la bonne gestion des risques TIC des entités (y compris dans le suivi des incidents). La CSSF indique que ces agents permettent ainsi d'assurer une gestion efficace des déclarations provenant des différentes catégories d'entités financières couvertes par DORA.

Comme pour l'ensemble de ses activités de supervision, la CSSF évalue régulièrement l'adéquation de ses ressources humaines et opérationnelles au regard de l'évolution de ses missions, du volume des notifications reçues et des besoins de surveillance identifiés.

16. **Le Ministre peut-il dresser un premier bilan qualitatif de l'application de DORA au Luxembourg depuis le 17 janvier 2025 ? Le niveau de préparation des entités financières luxembourgeoises est-il jugé satisfaisant ? Quels sont les principaux défis identifiés ?**

La CSSF constate une forte mobilisation de la place financière luxembourgeoise à la suite de l'entrée en application du cadre DORA, ainsi qu'une progression continue dans la mise en conformité des dispositifs internes ICT des entités concernées. Pour le surplus, il est renvoyé aux réponses détaillées fournies ci-dessus.

Luxembourg, le 3 juillet 2026

Le Ministre des Finances

(s.) Gilles Roth