JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2024 34

5 juin 2024

Orientations communes

Sur l'estimation des coûts et pertes annuels agrégés occasionnés par des incidents majeurs liés aux TIC au titre du règlement (UE) 2022/2554

Les présentes orientations comportent des références à des règlements délégués et d'exécution de la Commission européenne qui n'ont pas encore été publiés au Journal officiel de l'UE. Une fois que ces règlements auront été publiés au Journal officiel, les présentes orientations seront finalisées et incluront ces références. Les références seront insérées dans les sections surlignées en jaune.

La date de mise en application des présentes orientations ne pourra être déterminée qu'une fois celles-ci finalisées. La date prévue de mise en application des présentes orientations est le 17 janvier 2025. En cas de retard dans la finalisation des présentes orientations, le dernier jour de mise en application de celles-ci sera de deux mois à compter de la date de publication des traductions des orientations dans toutes les langues officielles de l'UE.

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Orientations communes sur l'estimation des coûts et pertes annuels agrégés occasionnés par des incidents majeurs liés aux TIC

Statut des présentes orientations communes

Le présent document comprend les orientations communes émises conformément aux dispositions des «règlements AES», à savoir à l'article 16 du règlement (UE) nº 1093/2010 [1], à l'article 16 du règlement (UE) nº 1094/2010 [2] et à l'article 16 du règlement (UE) nº 1095/2010 [3]. Conformément à l'article 16, paragraphe 3, de chacun des règlements AES, les autorités compétentes et les établissements financiers mettent tout en œuvre pour respecter ces orientations et recommandations.

Les orientations communes exposent le point de vue des AES sur les pratiques de surveillance appropriées au sein du système européen de surveillance financière ou sur la manière dont le droit de l'Union devrait être appliqué dans un domaine particulier. Les autorités compétentes auxquelles les orientations communes s'appliquent doivent s'y conformer en les intégrant dans leurs pratiques de surveillance, le cas échéant (par exemple, en modifiant leur cadre juridique ou leurs processus de surveillance), y compris lorsque les orientations communes s'adressent principalement aux établissements.

Obligations de déclaration

Conformément à l'article 16, paragraphe 3, des règlements AES, les autorités compétentes doivent indiquer à l'AES concernée si elles respectent ou entendent respecter ces orientations/recommandations communes ou, dans le cas contraire, indiquer les motifs de non-respect, au plus tard le 19.05.2025 (deux mois après l'émission). À défaut de notification dans ce délai, l'AES concernée considérera que les autorités compétentes ne respectent pas les orientations. Les notifications doivent être envoyées aux adresses compliance@eba.europa.eu, compliance@eiopa.europa.eu et DORA@esma.europa.eu, sous la référence «JC/GL/2024/34». Un modèle de notification est disponible sur les sites web des AES. Les notifications doivent être

[1] Règlement (UE) nº 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission *(JO L 331 du 15/12/2010, p. 12)*.

Règlement (UE) nº 1094/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/79/CE de la Commission *(JO L 331 du 15.12.2010, p. 48-83)*.

Règlement (UE) nº 1095/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des marchés financiers), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/77/CE de la Commission *(JO L 331 du 15.12.2010, p. 84-119)*.

communiquées par des personnes dûment habilitées à rendre compte du respect des orientations au nom des autorités compétentes qu'elles représentent.

Conformément à l'article 16, paragraphe 3, les notifications seront publiées sur les sites web des AES.

Titre I – Objet, champ d'application, destinataires et définitions

Objet et champ d'application

1. Les présentes orientations visent à remplir le mandat conféré aux AES en vertu de l'article 11, paragraphe 11, du règlement (UE) 2022/2554[4], à savoir élaborer des orientations communes sur l'estimation des coûts et pertes annuels agrégés occasionnés par des incidents majeurs liés aux TIC visés à l'article 11, paragraphe 10, dudit règlement. Les présentes orientations proposent également un modèle commun de présentation des coûts et pertes annuels agrégés.

Destinataires

2. Les présentes orientations s'adressent aux autorités compétentes telles que définies à l'article 46 du règlement (UE) 2022/2554 et aux établissements financiers tels que définis à l'article 4, paragraphe 1, du règlement (UE) nº 1093/2010, à l'article 4, paragraphe 1, du règlement (UE) nº 1094/2010 et à l'article 4, paragraphe 1, du règlement (UE) nº 1095/2010.

Définitions

3. Les termes utilisés et définis dans le règlement (UE) 2022/2554 ont la même signification dans les présentes orientations.

Titre II – Mise en œuvre

Date de mise en application

4. Les présentes orientations s'appliquent à compter du 19.05.2025.

Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) nº 2016/1011 *(JO L 333 du 27.12.2022, p. 1-79)*.

Titre III – Dispositions relatives à l'estimation des coûts et pertes annuels agrégés occasionnés par des incidents majeurs liés aux TIC

5. Les entités financières doivent estimer les coûts et les pertes annuels agrégés occasionnés par des incidents majeurs liés aux TIC en agrégeant les coûts et les pertes des incidents majeurs liés aux TIC qui relèvent de l'année de référence pour laquelle l'autorité compétente a sollicité l'estimation. L'entité financière peut choisir si l'année de référence correspond à l'année civile achevée ou à l'exercice comptable clos pour lequel l'entité financière a finalisé ses états financiers. Une fois qu'une entité financière a opté pour l'estimation sur la base de l'année civile ou de son exercice comptable, cette décision sera appliquée aux futures estimations des coûts et pertes annuels agrégés. L'entité financière peut modifier cette décision en informant l'autorité compétente, à condition que celle-ci ne s'y oppose pas dans un délai de deux mois à compter de la réception de la notification. Les entités financières ne doivent pas inclure les coûts et pertes liés aux incidents occasionnés avant ou après l'année de référence.

6. Les entités financières doivent inclure dans l'estimation tous les incidents liés aux TIC qui, quelle qu'en soit leur raison, ont été qualifiés de majeurs conformément au règlement délégué de la Commission [OJ L, 2024/1772, 25.6.2024][5] sur la classification des incidents et

   (a) pour lesquels l'entité financière a présenté un rapport définitif conformément à l'article 19, paragraphe 4, point c), du règlement (UE) 2022/2554 au cours de l'année de référence pertinente, ou

   (b) tout incident pour lequel l'entité financière a présenté, au cours des années de référence précédentes, un rapport définitif conformément à l'article 19, paragraphe 4, point c), du règlement (UE) 2022/2554, qui a eu une incidence financière quantifiable sur l'entité financière au cours de l'année de référence concernée.

7. Les entités financières doivent estimer les coûts et pertes annuels agrégés en appliquant les étapes successives suivantes:

   (a) estimer individuellement les coûts et les pertes de chaque incident majeur lié aux TIC, tel que visé au paragraphe 6. Ces estimations doivent montrer les coûts et pertes bruts compte tenu des types de coûts et de pertes visés à l'article 7, paragraphes 1 et 2, du règlement délégué de la Commission [OJ L, 2024/1772, 25.6.2024];

[5] Règlement délégué (UE) 2024/1772 de la Commission du 13 mars 2024 complétant le règlement (UE) 2022/2554 du Parlement européen et du Conseil par des normes techniques de réglementation précisant les critères de classification des incidents liés aux TIC et des cybermenaces, fixant des seuils d'importance significative et précisant les détails des rapports d'incidents majeurs, [*OJ L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj*]

(b) pour chaque incident majeur lié aux TIC, les entités financières doivent également estimer les recouvrements financiers tels qu'ils figurent à l'annexe II du règlement d'exécution de la Commission [*OJ L, 2025/302, 20.2.2025*][6];

(c) les entités financières doivent agréger les coûts et pertes bruts et les recouvrements financiers pour tous les incidents majeurs liés aux TIC.

8. Les entités financières doivent baser leurs estimations sur les coûts, pertes et recouvrements financiers reflétés dans leurs états financiers, tels que le compte de résultat, ou, le cas échéant, dans l'information prudentielle de l'année de référence pertinente. Dans leur estimation, les entités financières doivent également inclure les provisions comptables reflétées dans leurs états financiers, telles que le compte de résultat de l'année de référence pertinente. Lorsque des données exactes ne sont pas disponibles, les entités financières doivent, dans la mesure du possible, fonder leur estimation sur d'autres données et informations disponibles.

9. Les entités financières doivent inclure les ajustements des coûts et pertes de l'estimation présentée pour l'année précédente dans l'estimation de l'année de référence concernée, au cours de laquelle les ajustements seront effectués.

10. Les entités financières doivent également inclure, dans leur estimation des coûts et pertes annuels agrégés, la ventilation des coûts et pertes bruts et des recouvrements financiers pour chaque incident majeur lié aux TIC qui a été inclus dans l'agrégation.

11. Les entités financières doivent utiliser le modèle figurant en annexe pour soumettre à l'autorité compétente l'estimation de leurs coûts et pertes annuels agrégés pour l'année de référence. Pour chaque élément visé aux paragraphes 6 et 9 inclus dans l'estimation de l'année de référence, les entités financières doivent utiliser les mêmes codes de référence d'incident que ceux qu'elles ont utilisés dans le rapport définitif d'incident, conformément à l'article 19, paragraphe 4, point c), du règlement (UE) 2022/2554.

[6] Règlement d'exécution (UE) 2025/302 de la Commission du 23 octobre 2024 définissant des normes techniques d'exécution pour l'application du règlement (UE) 2022/2554 du Parlement européen et du Conseil en ce qui concerne les formulaires, modèles et procédures types permettant aux entités financières de notifier un incident majeur lié aux TIC et de notifier une cybermenace importante, [*OJ L, 2025/302, 20.2.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj*]

Annexe: Modèle de déclaration des coûts et pertes bruts et des recouvrements financiers de l'année de référence

Nom de l'entité financière				
Identifiant d'entité juridique (LEI)				
Dates de début et de fin de l'année de référence de l'entité financière				
Devise				
Nombre d'incidents	Date de soumission du rapport définitif d'incident	Numéro de référence de l'incident	Coûts et pertes bruts liés à l'incident au cours de l'année de référence (milliers d'unités)	Recouvrements de l'incident au cours de l'année de référence (milliers d'unités)
1				
2				
…				
Total pour l'année de référence	----------	----------		