Journal officiel
de l'Union européenne

FR
Série L

2025/302

20.2.2025

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

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le 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) 2016/1011 ([1]), et notamment son article 20, quatrième alinéa,

considérant ce qui suit:

(1) Afin que les entités financières déclarent les incidents majeurs à leurs autorités compétentes de manière cohérente et qu'elles fournissent auxdites autorités des données de bonne qualité, il convient de préciser les champs de données correspondant aux données que les entités financières doivent fournir aux différentes étapes de la déclaration prévue à l'article 19, paragraphe 4, du règlement (UE) 2022/2554. Il importe que ces informations soient présentées de manière que l'on puisse disposer d'une vue d'ensemble unique de l'incident. Il est donc nécessaire d'établir un modèle de déclaration unique à ces fins.

(2) Les entités financières devraient remplir les champs de données du modèle de déclaration qui correspondent aux exigences d'information applicables à la notification ou déclaration concernée. Toutefois, les entités financières qui disposent déjà d'informations qu'elles doivent fournir à un stade ultérieur de la déclaration, c'est-à-dire dans le rapport intermédiaire ou le rapport final, devraient être autorisées à anticiper la communication de ces données.

(3) Étant donné que des incidents multiples ou récurrents peuvent constituer un incident majeur au sens de l'article 8 du règlement délégué (UE) 2024/1772 de la Commission ([2]), la conception du modèle de déclaration et des champs de données devrait permettre aux entités financières de déclarer ces incidents récurrents.

(4) Afin que les informations soient exactes et à jour, le modèle de déclaration devrait permettre aux entités financières, lorsqu'elles soumettent le rapport intermédiaire et le rapport final, de mettre à jour toutes les informations qui ont été précédemment communiquées et, s'il y a lieu, de reclasser les incidents majeurs en incidents non majeurs.

(5) L'identification juridique des entités devrait être harmonisée avec les identifiants indiqués dans les normes techniques d'exécution adoptées en vertu de l'article 28, paragraphe 9, du règlement (UE) 2022/2554.

(6) Lorsque des entités financières externalisent auprès d'un tiers les obligations de déclaration des incidents majeurs liés aux TIC, les autorités compétentes devraient avoir connaissance de l'identité du tiers effectuant la déclaration au nom de l'entité financière avant que la première notification ou déclaration soit soumise, afin de vérifier la légitimité du tiers déclarant.

([1]) JO L 333 du 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) 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 (JO L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

(7) Pour mesurer facilement l'incidence d'un incident qui est survenu chez un prestataire tiers, ou a été causé par celui-ci, et qui touche plusieurs entités financières au sein d'un même État membre, ainsi que pour réduire l'effort de déclaration qui pèse sur les entités financières, le modèle de déclaration devrait permettre la soumission d'un rapport agrégé qui reprenne les informations agrégées concernant l'incidence de l'incident sur toutes les entités financières touchées qui ont classé l'incident comme majeur.

(8) Le modèle de déclaration devrait être conçu de manière neutre sur le plan technologique afin qu'il puisse être transposé dans diverses solutions de notification des incidents qui existent déjà ou qui peuvent être élaborées pour la mise en œuvre des exigences du règlement (UE) 2022/2554.

(9) La conception du modèle de déclaration et des champs de données devrait faciliter la notification des incidents majeurs liés aux TIC par les tiers auprès desquels des entités financières ont externalisé leur obligation de déclaration en vertu de l'article 19, paragraphe 5, du règlement (UE) 2022/2554.

(10) Le présent règlement se fonde sur le projet de normes techniques d'exécution soumis à la Commission par les autorités européennes de surveillance.

(11) Les autorités européennes de surveillance ont procédé à des consultations publiques ouvertes sur les projets de normes techniques d'exécution sur lesquels se fonde le présent règlement, en ont analysé les coûts et avantages potentiels et ont sollicité l'avis du groupe des parties intéressées au secteur bancaire institué par l'article 37 des règlements (UE) nº 1093/2010 ([3]), (UE) nº 1094/2010 ([4]) et (UE) nº 1095/2010 ([5]) du Parlement européen et du Conseil.

(12) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([6]) et a rendu un avis favorable le 22 juillet 2024. Tout traitement de données à caractère personnel relevant du champ d'application du présent règlement devrait être effectué conformément aux principes et dispositions applicables en matière de protection des données énoncés dans le règlement (UE) 2018/1725,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Modèle de déclaration des incidents majeurs liés aux TIC

1. Les entités financières utilisent le modèle figurant à l'annexe I pour soumettre la notification initiale, le rapport intermédiaire et le rapport final visés à l'article 19, paragraphe 4, du règlement (UE) 2022/2554, selon les modalités suivantes:

a) les entités financières qui soumettent une notification initiale remplissent les champs de données du modèle qui correspondent aux informations devant être fournies conformément à l'article 2 du règlement délégué (UE) 2025/301 de la Commission ([7]), et peuvent, lorsqu'elles disposent déjà de ces informations, compléter les champs de données qu'il n'est pas obligatoire de remplir pour les besoins d'une notification initiale mais qui doivent l'être pour la soumission d'un rapport intermédiaire ou final;

([3]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) Règlement délégué (UE) 2025/301 de la Commission du 23 octobre 2024 complétant le règlement (UE) 2022/2554 du Parlement européen et du Conseil par des normes techniques de réglementation précisant le contenu et les délais pour la notification initiale des incidents majeurs liés aux TIC, et pour les rapports intermédiaire et final y afférents, et le contenu de la notification volontaire en ce qui concerne les cybermenaces importantes (JO L, 2025/301, 20.2.2025, ELI: http://data.europa.eu/eli/reg_del/2025/301/oj).

b) les entités financières qui soumettent un rapport intermédiaire remplissent les champs de données du modèle qui correspondent aux informations devant être fournies conformément à l'article 3 du règlement délégué (UE) 2025/301, et peuvent, lorsqu'elles disposent déjà des informations pertinentes, compléter les champs de données qu'il n'est pas obligatoire de remplir pour les besoins du rapport intermédiaire mais qui doivent l'être pour la soumission du rapport final;

c) les entités financières qui soumettent un rapport final remplissent les champs de données du modèle qui correspondent aux informations devant être fournies conformément à l'article 4 du règlement délégué (UE) 2025/301

2. Les entités financières veillent à ce que les informations figurant dans la notification initiale ainsi que dans le rapport intermédiaire et le rapport final soient complètes et exactes.

3. Lorsque des données exactes ne sont pas disponibles au moment de soumettre la notification initiale ou le rapport intermédiaire, les entités financières fournissent, dans la mesure du possible, des valeurs estimées fondées sur d'autres données et informations disponibles.

4. Lorsqu'elles soumettent un rapport intermédiaire ou final, les entités financières utilisent le modèle figurant à l'annexe I pour communiquer toutes les informations requises et mettre à jour, s'il y a lieu, les informations précédemment fournies dans la notification initiale ou dans le rapport intermédiaire.

5. Lorsqu'elles remplissent le modèle figurant à l'annexe I, les entités financières se conforment au glossaire de données et aux instructions figurant à l'annexe II.

Article 2

Soumission conjointe de la notification initiale ainsi que des rapports intermédiaire et final

Les entités financières peuvent soumettre conjointement la notification initiale, le rapport intermédiaire et le rapport final afin de transmettre deux ou la totalité de ces documents simultanément, lorsque les activités régulières ont repris ou que l'analyse des causes originelles est terminée, et à condition que soient respectés les délais fixés à l'article 5 du règlement délégué (UE) 2025/301

Article 3

Incidents récurrents liés aux TIC

Les entités financières qui fournissent des informations sur les incidents récurrents non majeurs liés aux TIC qui remplissent cumulativement les conditions applicables à un incident majeur lié aux TIC énoncées à l'article 8, paragraphe 2, du règlement délégué (UE) 2024/1772 transmettent ces informations sous une forme agrégée.

Article 4

Utilisation de canaux électroniques sécurisés

1. Les entités financières utilisent des canaux électroniques sécurisés mis à disposition par leur autorité compétente pour soumettre la notification initiale et les rapports intermédiaire et final.

2. Les entités financières qui ne sont pas en mesure d'utiliser les canaux électroniques sécurisés mis à disposition par leur autorité compétente informent cette dernière d'un incident majeur lié aux TIC par d'autres moyens de communication sécurisés, en accord avec l'autorité compétente. Si l'autorité compétente l'exige, les entités financières soumettent à nouveau la notification initiale, ou le rapport intermédiaire ou final, par le canal électronique sécurisé mis à disposition par leur autorité compétente une fois qu'elles sont en mesure de le faire.

Article 5

Reclassement des incidents majeurs liés aux TIC

Si, à l'issue d'une évaluation complémentaire, l'entité financière conclut que l'incident lié aux TIC précédemment déclaré comme incident majeur ne remplissait à aucun moment les critères de classification ni n'atteignait les seuils visés à l'article 8 du règlement délégué (UE) 2024/1772, elle notifie à l'autorité compétente avoir reclassé l'incident lié aux TIC de majeur en incident non majeur en fournissant les informations relatives à ce reclassement au moyen du modèle figurant à l'annexe II du présent règlement en ce qui concerne les champs «type de soumission» et «autres informations».

Article 6

Notification de l'externalisation des obligations de déclaration

1. Les entités financières qui ont externalisé l'obligation de déclarer les incidents majeurs liés aux TIC en vertu de l'article 19, paragraphe 5, du règlement (UE) 2022/2554 informent leur autorité compétente de cet accord d'externalisation dès que celui-ci a été conclu et, au plus tard, avant la première notification ou déclaration.

2. Les entités financières communiquent à l'autorité compétente le nom, les coordonnées et le code d'identification du tiers qui soumettra, en leur nom, les notifications ou rapports d'incidents majeurs liés aux TIC.

3. Les entités financières informent leur autorité compétente dès qu'elles n'externalisent plus leurs obligations de déclaration selon l'article 19, paragraphe 5, du règlement (UE) 2022/2554.

Article 7

Déclaration agrégée

1. Un prestataire tiers de services auprès duquel des obligations de déclaration ont été externalisées conformément à l'article 19, paragraphe 5, du règlement (UE) 2022/2554 peut utiliser le modèle figurant à l'annexe I du présent règlement pour fournir, dans une seule et même notification ou un seul et même rapport, des informations agrégées sur un incident majeur lié aux TIC ayant une incidence sur plusieurs entités financières, et soumettre cette notification ou ce rapport à l'autorité compétente au nom de toutes les entités financières touchées, pour autant que toutes les conditions suivantes soient réunies:

a) l'incident majeur lié aux TIC devant être déclaré est imputable à un prestataire tiers de services TIC ou est causé par celui-ci;

b) ce prestataire tiers de services fournit le service TIC concerné à plus d'une entité financière ou à un groupe;

c) l'incident lié aux TIC est classé comme majeur par chaque entité financière mentionnée dans la notification agrégée ou le rapport agrégé;

d) l'incident majeur lié aux TIC touche des entités financières au sein d'un seul État membre et le rapport agrégé concerne des entités financières qui sont soumises à la surveillance de la même autorité compétente;

e) les autorités compétentes ont explicitement autorisé ce type d'entités financières à agréger leurs déclarations.

2. Le paragraphe 1 ne s'applique pas aux établissements de crédit jugés d'importance significative au sens de l'article 2, point 16), du règlement (UE) n° 468/2014 de la Banque centrale européenne ([8]), aux opérateurs de plates-formes de négociation et aux contreparties centrales, qui utilisent uniquement le modèle figurant à l'annexe I pour soumettre individuellement à leur autorité compétente des notifications ou des rapports d'incidents majeurs liés aux TIC.

3. Lorsque les autorités compétentes exigent des informations relatives à l'incidence individuelle de l'incident majeur lié aux TIC sur une seule et même entité financière, à la demande de l'autorité compétente, l'entité financière soumet une notification individuelle ou un rapport sur l'incident majeur lié aux TIC.

([8]) Règlement (UE) n° 468/2014 de la Banque centrale européenne du 16 avril 2014 établissant le cadre de la coopération au sein du mécanisme de surveillance unique entre la Banque centrale européenne, les autorités compétentes nationales et les autorités désignées nationales (le «règlement-cadre MSU») (BCE/2014/17) (JO L 141 du 14.5.2014, p. 1, ELI: http://data.europa.eu/eli/reg/2014/468/oj).

Article 8

Notification des cybermenaces importantes

1. Les entités financières qui notifient des cybermenaces importantes aux autorités compétentes conformément à l'article 19, paragraphe 2, du règlement (UE) 2022/2554 utilisent le modèle figurant à l'annexe III du présent règlement et se conforment au glossaire de données et aux instructions figurant à l'annexe IV du présent règlement.

2. Les entités financières veillent à ce que les informations figurant dans la notification des cybermenaces importantes soient complètes et exactes.

Article 9

Entrée en vigueur

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 23 octobre 2024.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE I

MODÈLES DE DÉCLARATION DES INCIDENTS MAJEURS LIÉS AUX TIC

Numéro du champ	Champ de données	
Informations générales relatives à l'entité financière		
1.1	Type de soumission	
1.2	Nom de l'entité soumettant le rapport	
1.3	Code d'identification de l'entité soumettant le rapport	
1.4	Type d'entité financière touchée	
1.5	Nom de l'entité financière touchée	
1.6	Code LEI de l'entité financière touchée	
1.7	Nom de la personne de contact principale	
1.8	Adresse électronique de la personne de contact principale	
1.9	Numéro de téléphone de la personne de contact principale	
1.10	Nom de la deuxième personne de contact	
1.11	Adresse électronique de la deuxième personne de contact	
1.12	Numéro de téléphone de la deuxième personne de contact	
1.13	Nom de la société mère ultime	
1.14	Code LEI de la société mère ultime	
1.15	Monnaie de déclaration	
Contenu de la notification initiale		
2.1	Code de référence de l'incident attribué par l'entité financière	
2.2	Date et heure de détection de l'incident majeur lié aux TIC	
2.3	Date et heure de classification de l'incident lié aux TIC comme majeur	
2.4	Description de l'incident majeur lié aux TIC	
2.5	Critères de classification donnant lieu à la déclaration d'incident	
2.6	Seuils d'importance significative pour le critère de classification «répartition géographique»	
2.7	Détection de l'incident majeur lié aux TIC	

Numéro du champ	Champ de données	
2.8	Mention indiquant si l'incident majeur lié aux TIC est imputable à un prestataire tiers ou à une autre entité financière	
2.9	Activation du plan de continuité des activités, s'il est activé	
2.10	Autres informations utiles	
Contenu du rapport intermédiaire		
3.1	Code de référence de l'incident attribué par l'autorité compétente	
3.2	Date et heure auxquelles l'incident majeur lié aux TIC est survenu	
3.3	Date et heure auxquelles les services, activités ou opérations ont repris	
3.4	Nombre des clients touchés	
3.5	Pourcentage de clients touchés	
3.6	Nombre des contreparties financières touchées	
3.7	Pourcentage de contreparties financières touchées	
3.8	Incidence sur les clients ou contreparties financières importants	
3.9	Nombre des transactions touchées	
3.10	Pourcentage de transactions touchées	
3.11	Valeur des transactions touchées	
3.12	Mention précisant si les chiffres sont réels ou sont des estimations, ou s'il n'y a pas eu d'incidence	
3.13	Atteinte à la réputation	
3.14	Informations contextuelles sur l'atteinte à la réputation	
3.15	Durée de l'incident majeur lié aux TIC	
3.16	Interruptions de service	
3.17	Mention précisant si les chiffres relatifs à la durée et à l'interruption de service sont réels ou sont des estimations	
3.18	Types d'incidence dans les États membres	
3.19	Description de la manière dont l'incident majeur lié aux TIC a une incidence dans d'autres États membres	
3.20	Seuils d'importance significative pour le critère de classification «pertes de données»	
3.21	Description des pertes de données	

Numéro du champ	Champ de données	
3.22	Critère de classification «services critiques touchés»	
3.23	Type d'incident majeur lié aux TIC	
3.24	Autres types d'incidents	
3.25	Menaces et techniques utilisées par l'acteur de la menace	
3.26	Autres types de techniques	
3.27	Informations sur les domaines fonctionnels et les processus opérationnels touchés	
3.28	Composants d'infrastructure touchés soutenant les processus opérationnels	
3.29	Informations sur les composants d'infrastructure touchés soutenant les processus opérationnels	
3.30	Incidence sur les intérêts financiers des clients	
3.31	Déclaration à d'autres autorités	
3.32	Indication des «autres» autorités	
3.33	Actions/mesures temporaires prises ou prévues pour le rétablissement après l'incident	
3.34	Description de toute action et mesure temporaire prise ou prévue pour le rétablissement après l'incident	
3.35	Indicateurs de compromis	
Contenu du rapport final		
4.1	Classification générale des causes originelles de l'incident	
4.2	Classification détaillée des causes originelles de l'incident	
4.3	Classification supplémentaire des causes originelles de l'incident	
4.4	Autres types de causes originelles	
4.5	Informations sur les causes originelles de l'incident	
4.6	Résumé de la résolution de l'incident	
4.7	Date et heure de traitement de la cause originelle de l'incident	
4.8	Date et heure de résolution de l'incident	
4.9	Informations indiquant si la date de résolution définitive de l'incident diffère de la date de mise en œuvre initialement prévue	
4.10	Évaluation des risques pour les fonctions critiques aux fins de la résolution	
4.11	Informations utiles aux autorités de résolution	

Numéro du champ	Champ de données	
4.12	Seuil d'importance significative pour le critère de classification «conséquences économiques»	
4.13	Montant des coûts et pertes directs et indirects bruts	
4.14	Montant des recouvrements financiers	
4.15	Mention précisant si les incidents non majeurs ont été récurrents	
4.16	Date et heure auxquelles les incidents récurrents sont survenus	

ANNEXE II

GLOSSAIRE DE DONNÉES ET INSTRUCTIONS POUR LA NOTIFICATION DES INCIDENTS MAJEURS

Champ de données		Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
Informations générales relatives à l'entité financière						
1.1.	Type de soumission	Indiquer le type de notification ou de rapport d'incident soumis à l'autorité compétente.	Oui	Oui	Oui	Choix: — notification initiale, — rapport intermédiaire, — rapport final, — incident majeur reclassé en incident non majeur.
1.2.	Nom de l'entité soumettant le rapport	Dénomination sociale complète de l'entité soumettant le rapport.	Oui	Oui	Oui	Alphanumérique
1.3.	Code d'identification de l'entité soumettant le rapport	Code d'identification de l'entité soumettant le rapport. Lorsque les entités financières soumettent la notification/le rapport, le code d'identification est l'identifiant d'entité juridique (LEI), code unique à 20 caractères alphanumériques conforme à la norme ISO 17442-1:2020. Un prestataire tiers qui soumet un rapport pour une entité financière peut utiliser un code d'identification tel que spécifié dans les normes techniques d'exécution adoptées en vertu de l'article 28, paragraphe 9, du règlement (UE) 2022/2554.	Oui	Oui	Oui	Alphanumérique
1.4.	Type de l'entité financière touchée	Type de l'entité, tel qu'énuméré à l'article 2, paragraphe 1, points a) à t), du règlement (UE) 2022/2554 pour laquelle le rapport est soumis. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, les différents types d'entités financières mentionnés dans le rapport agrégé doivent être sélectionnés.	Oui	Oui	Oui	Choix (sélection multiple): — les établissements de crédit, — les établissements de paiement, — les établissements de paiement exemptés, — les prestataires de services d'information sur les comptes, — les établissements de monnaie électronique, — les établissements de monnaie électronique exemptés, — les entreprises d'investissement, — les prestataires de services sur crypto-actifs, — les émetteurs de jetons se référant à un ou des actifs, — les dépositaires centraux de titres, — les contreparties centrales, — les plates-formes de négociation, — les référentiels centraux,

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
					— les gestionnaires de fonds d'investissement alternatifs, — les sociétés de gestion, — les prestataires de services de communication de données, — les entreprises d'assurance et de réassurance, — les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire, — les institutions de retraite professionnelle, — les agences de notation de crédit, — les administrateurs d'indices de référence d'importance critique, — les prestataires de services de financement participatif, — les référentiels des titrisations.
1.5. Nom de l'entité financière touchée	Dénomination sociale complète de l'entité financière touchée par l'incident majeur lié aux TIC et tenue de déclarer celui-ci à son autorité compétente en application de l'article 19 du règlement (UE) 2022/2554. En cas de déclaration agrégée: a) liste des noms de toutes les entités financières touchées par l'incident majeur lié aux TIC, séparés par un point-virgule; b) le prestataire tiers qui soumet une notification ou un rapport d'incident majeur sous la forme agrégée prévue à l'article 7 du présent règlement doit dresser la liste des noms de toutes les entités financières touchées par l'incident, séparés par un point-virgule.	Oui, si l'entité financière touchée par l'incident est différente de l'entité qui soumet le rapport et en cas de déclaration agrégée	Oui, si l'entité financière touchée par l'incident est différente de l'entité qui soumet le rapport et en cas de déclaration agrégée	Oui, si l'entité financière touchée par l'incident est différente de l'entité qui soumet le rapport et en cas de déclaration agrégée	Alphanumérique
1.6. Code LEI de l'entité financière touchée	Identifiant d'entité juridique (LEI) de l'entité financière touchée par l'incident majeur lié aux TIC attribué conformément aux normes établies par l'Organisation internationale de normalisation. En cas de déclaration agrégée: a) liste de tous les codes LEI des entités financières touchées par l'incident majeur lié aux TIC, séparés par un point-virgule;	Oui, si l'entité financière touchée par l'incident majeur lié aux TIC est	Oui, si l'entité financière touchée par l'incident majeur lié aux TIC est différente de l'entité qui	Oui, si l'entité financière touchée par l'incident majeur lié aux TIC est	Code unique à 20 caractères alphanumériques, conforme à la norme ISO 17442-1:2020

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
	b) le prestataire tiers qui soumet une notification ou un rapport d'incident majeur sous la forme agrégée prévue à l'article 7 du présent règlement doit dresser la liste des codes LEI de toutes les entités financières touchées par l'incident, séparés par un point-virgule. L'ordre dans lequel sont cités les codes LEI et les noms des entités financières est identique.	différente de l'entité qui soumet le rapport et en cas de déclaration agrégée	soumet le rapport et en cas de déclaration agrégée	différente de l'entité qui soumet le rapport et en cas de déclaration agrégée	
1.7. Nom de la personne de contact principale	Nom et prénom de la personne de contact principale de l'entité financière. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, nom de la personne de contact principale au sein de l'entité qui soumet le rapport agrégé.	Oui	Oui	Oui	Alphanumérique
1.8. Adresse électronique de la personne de contact principale	Adresse électronique de la personne de contact principale que l'autorité compétente peut utiliser pour la communication de suivi. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, adresse électronique de la personne de contact principale au sein de l'entité qui soumet le rapport agrégé.	Oui	Oui	Oui	Alphanumérique
1.9. Numéro de téléphone de la personne de contact principale	Numéro de téléphone de la personne de contact principale que l'autorité compétente peut utiliser pour la communication de suivi. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, numéro de téléphone de la personne de contact principale au sein de l'entité qui soumet le rapport agrégé. Le numéro de téléphone indiqué comporte tous les préfixes internationaux (par exemple +33 XXXXXXXXX).	Oui	Oui	Oui	Alphanumérique
1.10. Nom de la deuxième personne de contact	Nom et prénom de la deuxième personne de contact ou nom de l'équipe responsable de l'entité financière ou d'une entité qui soumet le rapport au nom de l'entité financière.	Oui	Oui	Oui	Alphanumérique
1.11. Adresse électronique de la deuxième personne de contact	Adresse électronique de la deuxième personne de contact ou adresse électronique fonctionnelle de l'équipe que l'autorité compétente peut utiliser pour la communication de suivi.	Oui	Oui	Oui	Alphanumérique

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
1.12. Numéro de téléphone de la deuxième personne de contact	Numéro de téléphone de la deuxième personne de contact, ou d'une équipe, que l'autorité compétente peut utiliser pour la communication de suivi. Le numéro de téléphone indiqué comporte tous les préfixes internationaux (par exemple +33 XXXXXXXXX).	Oui	Oui	Oui	Alphanumérique
1.13. Nom de la société mère ultime	Nom de la société mère ultime du groupe auquel appartient l'entité financière touchée, le cas échéant.	Oui, si l'entité financière appartient à un groupe	Oui, si l'entité financière appartient à un groupe	Oui, si l'entité financière appartient à un groupe	Alphanumérique
1.14. Code LEI de la société mère ultime	Code LEI de la société mère ultime du groupe auquel appartient l'entité financière touchée, le cas échéant. Attribué conformément aux normes établies par l'Organisation internationale de normalisation.	Oui, si l'entité financière appartient à un groupe	Oui, si l'entité financière appartient à un groupe	Oui, si l'entité financière appartient à un groupe	Code unique à 20 caractères alphanumériques, conforme à la norme ISO 17442-1:2020.
1.15. Monnaie de déclaration	Monnaie utilisée pour la déclaration de l'incident	Oui	Oui	Oui	Choix effectué en utilisant les codes monnaie de la norme ISO 4217
Contenu de la notification initiale					
2.1. Code de référence de l'incident attribué par l'entité financière	Code de référence unique délivré par l'entité financière identifiant sans équivoque l'incident majeur lié aux TIC. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, code de référence de l'incident attribué par le prestataire tiers.	Oui	Oui	Oui	Alphanumérique
2.2. Date et heure de détection de l'incident lié aux TIC	Date et heure auxquelles l'entité financière a pris connaissance de l'incident lié aux TIC. Pour les incidents récurrents, date et heure auxquelles le dernier incident lié aux TIC a été détecté.	Oui	Oui	Oui	Norme ISO 8601 TUC (aaaa-mm-jj hh: mm:ss)

Champ de données		Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
2.3.	Date et heure auxquelles l'incident a été classé comme majeur	Date et heure auxquelles l'incident lié aux TIC a été classé comme majeur conformément aux critères de classification établis dans le règlement délégué (UE) 2024/1772.	Oui	Oui	Oui	Norme ISO 8601 TUC (aaaa-mm-jj hh: mm:ss)
2.4.	Description de l'incident lié aux TIC	Description des aspects les plus pertinents de l'incident majeur lié aux TIC. Les entités financières fournissent un aperçu schématique des informations suivantes: causes possibles, incidences immédiates, systèmes concernés, etc. Les entités financières indiquent, lorsque ces informations sont connues ou devraient raisonnablement l'être, si l'incident a une incidence sur les prestataires tiers ou d'autres entités financières, le type de prestataire ou d'entité financière, leur nom, leurs codes d'identification respectifs et le type de code d'identification (par exemple, LEI ou EUID). Dans les rapports ultérieurs, le contenu de ce champ peut évoluer au fil du temps pour qu'en ressorte à tout moment la compréhension de l'incident lié aux TIC et pour qu'y soit consignée toute autre information pertinente concernant ce dernier qui n'est pas couverte par les champs de données, y compris l'évaluation interne de la gravité par l'entité financière (par exemple, très faible, faible, moyenne, élevée, très élevée) ainsi que le niveau et le nom des structures décisionnelles les plus élevées qui ont participé à la réaction à l'incident lié aux TIC.	Oui	Oui	Oui	Alphanumérique
2.5.	Critères de classification donnant lieu à la déclaration d'incident	Critères de classification au titre du règlement délégué (UE) 2024/1772 selon lesquels l'incident lié aux TIC a été qualifié de majeur et qui ont donné lieu à la notification et aux rapports ultérieurs. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, critères de classification selon lesquels l'incident lié aux TIC a été qualifié de majeur pour au moins une ou plusieurs entités financières.	Oui	Oui	Oui	Choix (plusieurs réponses possibles): — clients, contreparties financières et transactions touchés, — atteinte à la réputation, — durée et interruptions de service, — répartition géographique, — pertes de données, — services critiques touchés, — conséquences économiques.
2.6.	Seuils d'importance significative pour le critère de classification «répartition géographique»	États membres de l'EEE touchés par l'incident majeur lié aux TIC Lorsqu'elles évaluent l'incidence de l'incident majeur lié aux TIC dans d'autres États membres, les entités financières tiennent compte des articles 4 et 12 du règlement délégué (UE) 2024/1772.	Oui, si le critère «répartition géographique» est rempli	Oui, si le critère «répartition géographique» est rempli	Oui, si le critère «répartition géographique» est rempli	Choix (plusieurs réponses possibles) effectué en utilisant la norme ISO 3166 ALPHA-2 des pays touchés

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
2.7. Détection de l'incident majeur lié aux TIC	Indication de la manière dont l'incident majeur lié aux TIC a été détecté.	Oui	Oui	Oui	Choix: — sécurité informatique, — personnel, — audit interne, — audit externe, — clients, — contreparties financières, — prestataire tiers, — agresseur, — systèmes de surveillance, — autorité/agence/organe répressif, — autres.
2.8. Mention précisant si l'incident est imputable à un prestataire tiers ou à une autre entité financière	Mention précisant si l'incident majeur lié aux TIC est imputable à un prestataire tiers ou à une autre entité financière. Les entités financières indiquent si l'incident majeur lié aux TIC est imputable à un prestataire tiers ou à une autre entité financière (y compris les entités financières appartenant au même groupe que l'entité déclarante), ainsi que le nom, le code d'identification du prestataire tiers ou de l'entité financière et le type de code d'identification (par exemple, LEI ou EUID).	Oui, si l'incident est imputable à un prestataire tiers ou à une autre entité financière	Oui, si l'incident est imputable à un prestataire tiers ou à une autre entité financière	Oui, si l'incident est imputable à un prestataire tiers ou à une autre entité financière	Alphanumérique
2.9. Activation du plan de continuité des activités, s'il est activé	Mention précisant si les mesures de réponse visant à assurer la continuité des activités de l'entité financière ont été formellement activées.	Oui	Oui	Oui	Booléen (oui ou non)
2.10. Autres informations utiles	Toute autre information non reprise dans le modèle. Les entités financières qui ont reclassé un incident majeur lié aux TIC en incident non majeur exposent les raisons pour lesquelles cet incident ne remplit pas, et ne devrait pas remplir, les critères pour être considéré comme un incident majeur lié aux TIC.	Oui, s'il existe d'autres informations non reprises dans le	Oui, s'il existe d'autres informations non reprises dans le modèle ou si l'incident	Oui, s'il existe d'autres informations non reprises dans le modèle	Alphanumérique

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
		modèle ou si l'incident majeur lié aux TIC a été reclassé en incident non majeur	majeur lié aux TIC a été reclassé en incident non majeur	ou si l'incident majeur lié aux TIC a été reclassé en incident non majeur	
Contenu du rapport intermédiaire					
3.1. Code de référence de l'incident attribué par l'autorité compétente	Code de référence unique attribué par l'autorité compétente au moment de la réception de la notification initiale pour identifier sans équivoque l'incident majeur lié aux TIC.	Non	Oui, le cas échéant	Oui, le cas échéant	Alphanumérique
3.2. Date et heure auxquelles l'incident est survenu	Date et heure auxquelles l'incident majeur lié aux TIC est survenu, si elles diffèrent du moment où l'entité financière en a pris connaissance. Pour les incidents majeurs récurrents liés aux TIC, date et heure auxquelles s'est produit le dernier incident majeur lié aux TIC.	Non	Oui	Oui	Norme ISO 8601 TUC (aaaa-mm-jj hh: mm:ss)
3.3. Date et heure auxquelles les services, activités ou opérations ont repris	Informations sur la date et l'heure auxquelles les services, activités ou opérations touchés par l'incident majeur lié aux TIC ont repris.	Non	Oui, si le champ de données 3.16 «Interruptions de service» a été rempli	Oui, si le champ de données 3.16 «Interruptions de service» a été rempli	Norme ISO 8601 TUC (aaaa-mm-jj hh: mm:ss)
3.4. Nombre des clients touchés	Nombre des clients touchés par l'incident majeur lié aux TIC qui utilisent le service fourni par l'entité financière. Lorsqu'elles évaluent le nombre des clients touchés, les entités financières tiennent compte, dans leur évaluation, de l'article 1er, paragraphe 1, et de l'article 9, paragraphe 1, point b), du règlement délégué (UE) 2024/1772. Une entité financière qui n'est pas en mesure de déterminer le nombre réel des clients touchés utilise des estimations établies à partir des données disponibles portant sur des périodes de référence comparables. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, nombre total des clients touchés pour l'ensemble des entités financières.	Non	Oui	Oui	Nombre entier

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
3.5. Pourcentage de clients touchés	Pourcentage de clients touchés par l'incident majeur lié aux TIC par rapport au nombre total de clients qui utilisent le service touché fourni par l'entité financière. Dans le cas où plusieurs services seraient touchés, les services sont fournis de manière agrégée. Les entités financières tiennent compte, dans leur évaluation, de l'article 1er, paragraphe 1, et de l'article 9, paragraphe 1, point a), du règlement délégué (UE) 2024/1772. Une entité financière qui ne peut pas déterminer le pourcentage réel de clients touchés utilise des estimations établies à partir des données disponibles portant sur des périodes de référence comparables. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, une entité financière divise la somme de tous les clients touchés par le nombre total des clients de toutes les entités financières touchées.	Non	Oui	Oui	Exprimé en pourcentage — toute valeur jusqu'à 5 caractères numériques, dont 1 décimale au maximum, exprimée en pourcentage (par exemple 2,4 au lieu de 2,4 %). Si la valeur comporte plus de 1 chiffre après le séparateur décimal, les contreparties déclarantes arrondissent à la moitié supérieure.
3.6. Nombre des contreparties financières touchées	Nombre des contreparties financières touchées par l'incident majeur lié aux TIC qui ont conclu un contrat avec l'entité financière. Lorsqu'elles évaluent le nombre des contreparties financières touchées, les entités financières tiennent compte, dans leur évaluation, de l'article 1er, paragraphe 2, du règlement délégué (UE) 2024/1772. Une entité financière qui ne peut pas déterminer le nombre réel des contreparties financières touchées utilise des estimations établies à partir des données disponibles portant sur des périodes de référence comparables. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, nombre total des contreparties financières touchées pour l'ensemble des entités financières.	Non	Oui	Oui	Nombre entier

Champ de données		Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
3.7.	Pourcentage de contreparties financières touchées	Pourcentage de contreparties financières touchées par l'incident majeur lié aux TIC par rapport au nombre total de contreparties financières ayant conclu un contrat avec l'entité financière. Lors de l'évaluation du pourcentage de contreparties financières touchées, les entités financières tiennent compte, dans leur évaluation, de l'article 1er, paragraphe 1, et de l'article 9, paragraphe 1, point c), du règlement délégué (UE) 2024/1772. Une entité financière qui ne peut pas déterminer le pourcentage réel de contreparties financières touchées utilise des estimations établies à partir des données disponibles portant sur des périodes de référence comparables. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, indiquer la somme de toutes les contreparties financières touchées divisée par le nombre total des contreparties financières de toutes les entités financières touchées.	Non	Oui	Oui	Exprimé en pourcentage — toute valeur jusqu'à 5 caractères numériques, dont 1 décimale au maximum, exprimée en pourcentage (par exemple 2,4 au lieu de 2,4 %). Si la valeur comporte plus de 1 chiffre après le séparateur décimal, les contreparties déclarantes arrondissent à la moitié supérieure.
3.8.	Incidence sur les clients ou contreparties financières importants	Toute incidence constatée sur les clients ou les contreparties financières importants visés à l'article 1er, paragraphe 3, et à l'article 9, paragraphe 1, point f), du règlement délégué (UE) 2024/1772.	Non	Oui, si le seuil «importance des clients et des contreparties financières» est atteint	Oui, si le seuil «importance des clients et des contreparties financières» est atteint	Booléen (oui ou non)
3.9.	Nombre des transactions touchées	Nombre des transactions touchées par l'incident majeur lié aux TIC. Lorsqu'elles évaluent l'incidence sur les transactions, les entités financières tiennent compte de l'article 1er, paragraphe 4, du règlement délégué (UE) 2024/1772, y compris de toutes les transactions nationales et transfrontières touchées impliquant un montant monétaire qui sont au moins en partie effectuées dans l'Union.	Non	Oui, si une transaction a été touchée par l'incident	Oui, si une transaction a été touchée par l'incident	Nombre entier

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
	Une entité financière qui ne peut pas déterminer le nombre réel des transactions touchées utilise des estimations établies à partir des données disponibles portant sur des périodes de référence comparables. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, indiquer le nombre total de transactions touchées pour l'ensemble des entités financières.				
3.10. Pourcentage de transactions touchées	Pourcentage de transactions touchées par rapport au nombre moyen journalier de transactions nationales et transfrontières effectuées par l'entité financière liées au service touché. Les entités financières tiennent compte de l'article 1er, paragraphe 4, et de l'article 9, paragraphe 1, point d), du règlement délégué (UE) 2024/1772. Une entité financière qui ne peut pas déterminer le pourcentage réel des transactions touchées utilise des estimations. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, une entité financière additionne le nombre de toutes les transactions touchées et divise cette somme par le nombre total des transactions de toutes les entités financières touchées.	Non	Oui, si une transaction a été touchée par l'incident	Oui, si une transaction a été touchée par l'incident	Exprimé en pourcentage — toute valeur jusqu'à 5 caractères numériques, dont 1 décimale au maximum, exprimée en pourcentage (par exemple 2,4 au lieu de 2,4 %). Si la valeur comporte plus de 1 chiffre après le séparateur décimal, les contreparties déclarantes arrondissent à la moitié supérieure.
3.11. Valeur des transactions touchées	La valeur totale des transactions touchées par l'incident majeur lié aux TIC est évaluée conformément à l'article 1er, paragraphe 4, et à l'article 9, paragraphe 1, point e), du règlement délégué (UE) 2024/1772. Une entité financière qui ne peut pas déterminer la valeur réelle des transactions touchées utilise des estimations établies à partir des données disponibles portant sur des périodes de référence comparables. Une entité financière déclare le montant monétaire comme une valeur positive. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, indiquer la valeur totale des transactions touchées pour toutes les entités financières.	Non	Oui, si une transaction a été touchée par l'incident	Oui, si une transaction a été touchée par l'incident	Monétaire Les entités financières déclarent le point de données en unités avec une précision minimale fixée au millier d'unités (par exemple 2,5 au lieu de 2 500 EUR).

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
3.12. Mention précisant si les chiffres sont réels ou sont des estimations	Mention précisant si les valeurs déclarées dans les champs de données 3.4 à 3.11 sont réelles ou sont des estimations, ou s'il n'y a pas eu d'incidence.	Non	Oui	Oui	Choix (plusieurs réponses possibles): — chiffres réels pour les clients touchés, — chiffres réels pour les contreparties financières touchées, — chiffres réels pour les transactions touchées, — estimations pour les clients touchés, — estimations pour les contreparties financières touchées, — estimations pour les transactions touchées, — aucune incidence sur les clients, — aucune incidence sur les contreparties financières, — aucune incidence sur les transactions.
3.13. Atteinte à la réputation	Informations sur l'incidence de l'incident majeur lié aux TIC sur la réputation, telle que prévue aux articles 2 et 10 du règlement délégué (UE) 2024/1772. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, indiquer les catégories d'atteintes à la réputation qui s'appliquent à au moins une entité financière.	Non	Oui, si le critère «atteinte à la réputation» est rempli	Oui, si le critère «atteinte à la réputation» est rempli	Choix (plusieurs réponses possibles): — l'incident majeur lié aux TIC a été relayé par les médias, — l'incident majeur lié aux TIC a donné lieu à des plaintes répétées de la part de différents clients ou contreparties financières concernant des services en contact direct avec la clientèle ou des relations commerciales critiques, — l'entité financière ne pourra pas satisfaire à certaines exigences réglementaires, ou il est probable qu'elle ne le pourra pas, en raison de l'incident majeur lié aux TIC, — l'entité financière perdra, ou il est probable qu'elle perdra, des clients ou des contreparties financières en raison de l'incident majeur lié aux TIC, au grand détriment de son activité.
3.14. Informations contextuelles sur l'atteinte à la réputation	Informations expliquant comment l'incident majeur lié aux TIC a porté, ou pourrait porter, atteinte à la réputation de l'entité financière, y compris les infractions à la loi, les exigences réglementaires non respectées, le nombre de plaintes de clients, etc.	Non	Oui, si le critère «atteinte à la réputation» est rempli	Oui, si le critère «atteinte à la réputation» est rempli	Alphanumérique

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
	Les informations contextuelles comprennent le type de médias (par exemple, médias traditionnels et numériques, blogs, plateformes de diffusion en continu) et la couverture médiatique, y compris la portée des médias (locale, nationale, internationale). Ne relèvent pas d'une couverture médiatique dans ce contexte les quelques commentaires négatifs d'abonnés ou d'utilisateurs de réseaux sociaux. L'entité financière indique également si la couverture médiatique a mis en évidence des risques importants pour ses clients liés à l'incident majeur lié aux TIC, y compris le risque d'insolvabilité de l'entité financière ou le risque de perte de fonds. Les entités financières indiquent également si elles ont communiqué aux médias des éléments permettant d'informer de manière fiable le public de l'incident majeur lié aux TIC et de ses conséquences. Les entités financières peuvent également indiquer si de fausses informations ont circulé dans les médias en ce qui concerne l'incident lié aux TIC, y compris des informations fondées sur la propagation délibérée de fausses informations par des acteurs de la menace, ou des informations relatives à la dégradation du site web de l'entité financière ou illustrant cette dégradation.				
3.15. Durée de l'incident	Les entités financières mesurent la durée de l'incident majeur lié aux TIC à partir du moment où l'incident est survenu jusqu'au moment où il est résolu. Les entités financières qui ne sont pas en mesure de déterminer le moment auquel l'incident majeur lié aux TIC est survenu mesurent la durée de l'incident entre le moment où l'entité financière a détecté l'incident et celui où elle l'a enregistré dans les journaux des réseaux ou des systèmes ou dans d'autres sources de données, le moment le plus proche étant retenu. Les entités financières qui ne savent pas encore quand l'incident majeur lié aux TIC sera résolu appliquent des estimations. La valeur est exprimée en jours, heures et minutes. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, les entités financières mesurent la durée la plus longue de l'incident majeur lié aux TIC en cas de différences entre les entités financières.	Non	Oui	Oui	jj:hh:mm

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
3.16. Interruptions de service	Les interruptions de service sont mesurées à partir du moment où le service est totalement ou partiellement indisponible pour les clients, les contreparties financières ou d'autres utilisateurs internes ou externes jusqu'au moment où les activités ou opérations régulières ont repris au niveau de service qui était fourni avant l'incident majeur lié aux TIC. Lorsque l'interruption de service provoque un retard dans la fourniture d'un service après la reprise des activités ou opérations régulières, les entités financières mesurent l'interruption à partir du début de l'incident majeur lié aux TIC jusqu'au moment où le service ayant subi un retard est fourni. Les entités financières qui ne sont pas en mesure de déterminer le moment auquel l'interruption de service a commencé, mesurent l'interruption de service entre le moment où l'incident a été détecté et celui où il a été enregistré, le moment le plus proche étant retenu. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, les entités financières mesurent, en cas de différences entre les entités financières, la durée la plus longue de l'interruption de service.	Non	Oui, si l'incident a provoqué une interruption de service	Oui, si l'incident a provoqué une interruption de service	jj:hh:mm
3.17. Mention précisant si les chiffres relatifs à la durée et à l'interruption de service sont réels ou sont des estimations.	Mention précisant si les valeurs déclarées dans les champs de données 3.15 et 3.16 sont réelles ou sont des estimations.	Non	Oui, si le critère «durée et interruptions de service» est rempli	Oui, si le critère «durée et interruptions de service» est rempli	Choix: — chiffres réels, — estimations, — chiffres réels et estimations, — aucune information disponible.
3.18. Types d'incidence dans les États membres	Type d'incidence dans les différents États membres de l'EEE. Mention précisant si l'incident majeur lié aux TIC a eu une incidence dans d'autres États membres de l'EEE (autres que l'État membre de l'autorité compétente à laquelle l'incident est directement déclaré), conformément à l'article 4 du règlement délégué (UE) 2024/1772, et notamment l'importance de cette incidence en ce qui concerne: a) les clients et les contreparties financières touchés dans d'autres États membres; ou	Non	Oui, si le critère «répartition géographique» est rempli	Oui, si le critère «répartition géographique» est rempli	Choix (plusieurs réponses possibles): — clients, — contreparties financières, — succursale de l'entité financière, — entités financières du groupe qui exercent des activités dans l'État membre concerné, — infrastructure des marchés financiers, — prestataires tiers qui peuvent être communs à d'autres entités financières.

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
	b) les succursales ou les autres entités financières du groupe qui exercent des activités dans d'autres États membres; ou c) les infrastructures des marchés financiers ou les prestataires tiers susceptibles d'affecter les entités financières établies dans d'autres États membres auxquelles ils fournissent des services.				
3.19. Description de l'incidence de l'incident dans d'autres États membres	Description de l'incidence et de la gravité de l'incident majeur lié aux TIC dans chaque État membre touché, y compris évaluation de l'incidence et de la gravité sur: a) les clients; b) les contreparties financières; c) les succursales de l'entité financière; d) les autres entités financières du groupe qui exercent des activités dans l'État membre concerné; e) les infrastructures des marchés financiers; f) les prestataires tiers qui peuvent être communs à d'autres entités financières, le cas échéant, dans un ou plusieurs autres États membres.	Non	Oui, si le critère «répartition géographique» est rempli	Oui, si le critère «répartition géographique» est rempli	Alphanumérique
3.20. Seuils d'importance significative pour le critère de classification «pertes de données»	Type de pertes de données occasionnées par l'incident majeur lié aux TIC en ce qui concerne la disponibilité, l'authenticité, l'intégrité et la confidentialité des données. Les entités financières tiennent compte, dans leur évaluation, des articles 5 et 13 du règlement délégué (UE) 2024/1772. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, indiquer les pertes de données touchant au moins une entité financière.	Non	Oui, si le critère «pertes de données» est rempli	Oui, si le critère «pertes de données» est rempli	Choix (plusieurs réponses possibles): — disponibilité, — authenticité, — intégrité, — confidentialité.
3.21. Description des pertes de données	Description de l'incidence de l'incident majeur lié aux TIC sur la disponibilité, l'authenticité, l'intégrité et la confidentialité des données critiques conformément aux articles 5 et 13 du règlement délégué (UE) 2024/1772. Informations concernant l'incidence sur la mise en œuvre des objectifs opérationnels de l'entité financière ou sur le respect des exigences réglementaires. Dans les informations communiquées, les entités financières indiquent si les données touchées sont des données de clients, des données d'autres entités (par exemple, les contreparties financières) ou des données de l'entité financière elle-même.	Non	Oui, si le critère «pertes de données» est rempli	Oui, si le critère «pertes de données» est rempli	Alphanumérique

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
	L'entité financière peut également indiquer le type de données concernées par l'incident — en particulier, si les données sont confidentielles et le type de confidentialité concerné (par exemple, secret commercial/secret des affaires, données à caractère personnel, secret professionnel: secret bancaire, secret des assurances, secret des services de paiement, etc.). Ces informations peuvent également inclure les risques éventuels associés aux pertes de données, par exemple le fait que les données touchées par l'incident puissent être utilisées pour identifier des personnes et que l'acteur de la menace puisse s'en servir pour obtenir des crédits ou des prêts sans leur consentement, pour commettre des attaques d'hameçonnage ciblé ou pour divulguer des informations au public. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, description générale de l'incidence de l'incident sur les entités financières touchées. Lorsque cette incidence est différenciée, l'incidence particulière sur les différentes entités financières est clairement indiquée dans la description.				
3.22. Critère de classification «services critiques touchés»	Informations relatives au critère «services critiques touchés». Les entités financières tiennent compte, dans leur évaluation, de l'article 6 du règlement délégué (UE) 2024/1772, y compris des informations sur: — les services ou activités touchés qui nécessitent un agrément ou un enregistrement ou qui sont surveillés par les autorités compétentes, ou — les services TIC ou les réseaux et les systèmes d'information qui soutiennent des fonctions critiques ou importantes de l'entité financière, et — la nature de l'accès malveillant et non autorisé aux réseaux et aux systèmes d'information de l'entité financière. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, indiquer l'incidence sur les services critiques qui s'appliquent à au moins une entité financière.	Non	Oui	Oui	Alphanumérique

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
3.23. Type d'incident	Classification des incidents par type.	Non	Oui	Oui	Choix (plusieurs réponses possibles): — lié à la cybersécurité, — défaillance de processus, — défaillance des systèmes, — événement extérieur, — lié aux paiements, — autres (veuillez préciser).
3.24. Autres types d'incidents	Autres types d'incidents majeurs liés aux TIC: les entités financières qui ont sélectionné «autres» types d'incident dans le champ de données 3.23 précisent le type d'incident lié aux TIC.	Non	Oui, si «autres» types d'incident est sélectionné dans le champ de données 3.23	Oui, si «autres» types d'incident est sélectionné dans le champ de données 3.23	Alphanumérique
3.25. Menaces et techniques utilisées par l'acteur de la menace	Indiquer les menaces et les techniques utilisées par l'acteur de la menace, notamment: a) ingénierie sociale, y compris hameçonnage; b) attaque par déni de service distribué (DDoS); c) usurpation d'identité; d) chiffrement de données aux fins de leur destruction (data encryption for impact), y compris rançongiciels; e) détournement de ressources; f) exfiltration et manipulation de données, à l'exclusion de l'usurpation d'identité; g) destruction de données; h) défacement; i) attaque de la chaîne d'approvisionnement; j) autres (veuillez préciser).	Non	Oui, si le type d'incident lié aux TIC «lié à la cybersécurité» est sélectionné dans le champ 3.23	Oui, si le type d'incident lié aux TIC «lié à la cybersécurité» est sélectionné dans le champ 3.23	Choix (plusieurs réponses possibles): — ingénierie sociale (y compris hameçonnage), — attaque par déni de service distribué (DDoS), — usurpation d'identité, — chiffrement de données aux fins de leur destruction (data encryption for impact), y compris rançongiciels, — détournement de ressources, — exfiltration et manipulation de données, y compris usurpation d'identité, — destruction de données, — défacement, — attaque de la chaîne d'approvisionnement, — autres (veuillez préciser).
3.26. Autres types de techniques	Autres types de techniques Les entités financières qui ont sélectionné «autres» types de techniques dans le champ de données 3.25 précisent le type de technique utilisée.	Non	Oui, si «autres» types de techniques est sélectionné dans le champ de données 3.25	Oui, si «autres» types de techniques est sélectionné dans le champ de données 3.25	Alphanumérique

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
3.27. Informations sur les domaines fonctionnels et les processus opérationnels touchés	Indication des domaines fonctionnels et des processus opérationnels qui sont touchés par l'incident, y compris les produits et services. Les domaines fonctionnels comprennent, sans s'y limiter: a) les activités de marketing et le développement commercial; b) le service à la clientèle; c) la gestion des produits; d) le respect des dispositions réglementaires; e) la gestion des risques; f) les finances et la comptabilité; g) les RH et les services généraux; h) les technologies de l'information. Les processus opérationnels comprennent, sans s'y limiter: — l'information sur les comptes, — les services des actuaires, — l'acquisition d'opérations de paiement, — l'authentification/autorisation, — l'autorité, — l'entrée en relation avec le client, — l'administration des prestations, — la gestion du paiement des prestations, — l'achat et la vente de contrats d'assurance à forfait entre société d'assurances, — les paiements par carte, — la gestion de la caisse, — le placement ou le retrait d'espèces, — la gestion des créances d'assurance, — la procédure de demande d'indemnités assurance, — la compensation, — les conglomérats de prêts aux entreprises, — les assurances collectives, — les virements, — la garde et la conservation d'actifs, — l'entrée en relation avec un client, — l'ingestion de données, — le traitement de données, — les prélèvements, — les assurances à l'exportation, — la finalisation des opérations/transactions, — le placement d'instruments financiers, — la comptabilité de fonds,	Non	Oui	Oui	Alphanumérique

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
	— le change de devises, — le conseil en investissement, — la gestion d'investissements, — l'émission d'instruments de paiement, — la gestion des prêts, — les modalités de paiement de l'assurance-vie, — les transmissions de fonds, — le calcul de l'actif net, — les ordres, — l'initiation de paiements, — la souscription d'assurances, — la gestion de portefeuille, — la perception des primes, — la réception/la transmission/l'exécution, — la réassurance, — le règlement, — le suivi des transactions. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, indiquer les domaines fonctionnels et processus opérationnels touchés dans au moins une entité financière.				
3.28. Composants d'infrastructure touchés soutenant les processus opérationnels	Informations précisant si l'incident majeur lié aux TIC a touché les composants d'infrastructure (serveurs, systèmes d'exploitation, logiciels, serveurs d'application, logiciels intermédiaires, composants de réseau, autres) soutenant les processus opérationnels.	Non	Oui	Oui	Choix: — oui, — non, — informations non disponibles.
3.29. Informations sur les composants d'infrastructure touchés soutenant les processus opérationnels	Description de l'incidence de l'incident majeur lié aux TIC sur les composants d'infrastructure soutenant les processus opérationnels, y compris le matériel et les logiciels. Le matériel comprend les serveurs, ordinateurs, centres de données, commutateurs, routeurs et plateformes. Les logiciels comprennent les systèmes d'exploitation, applications, bases de données, outils de sécurité, composants de réseau, autres (veuillez préciser). Dans les descriptions, il convient de décrire ou de désigner les composants ou systèmes d'infrastructure touchés et de fournir, s'ils sont disponibles, les renseignements suivants: a) les informations sur la version; b) l'infrastructure interne/partiellement externalisée/entièrement externalisée — nom du prestataire tiers;	Non	Oui, si l'incident a touché des composants d'infrastructure soutenant les processus opérationnels	Oui, si l'incident a touché des composants d'infrastructure soutenant les processus opérationnels	Alphanumérique

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
	c) si l'infrastructure est utilisée ou partagée entre plusieurs fonctions opérationnelles; d) les dispositions pertinentes prises en matière de résilience/continuité/rétablissement/substituabilité.				
3.30. Incidence sur les intérêts financiers des clients	Informations indiquant si l'incident majeur lié aux TIC a eu une incidence sur les intérêts financiers des clients.	Non	Oui	Oui	Choix: — oui, — non, — informations non disponibles.
3.31. Déclaration à d'autres autorités	Mention des autorités qui ont été informées de l'incident majeur lié aux TIC. Compte tenu des différences résultant de la législation nationale des États membres, on entend par autorités répressives les entités financières au sens large pour y inclure les autorités publiques, y compris la police, les forces de l'ordre et les procureurs, habilitées à poursuivre les auteurs d'actes de cybercriminalité.	Non	Oui	Oui	Choix (plusieurs réponses possibles): — police/services répressifs, — CSIRT, — Autorité chargée de la protection des données, — Agence nationale de cybersécurité, — aucune, — autres (veuillez préciser).
3.32. Indication des «autres» autorités	Indication des «autres» types d'autorités informées de l'incident majeur lié aux TIC. Si l'option «autres» a été sélectionnée dans le champ de données 3.31, la description comprend des informations plus détaillées sur l'autorité à laquelle l'entité financière a communiqué des informations relatives à l'incident majeur lié aux TIC.	Non	Oui, si un «autre» type d'autorité a été informé par l'entité financière de l'incident majeur lié aux TIC	Oui, si un «autre» type d'autorité a été informé par l'entité financière de l'incident majeur lié aux TIC	Alphanumérique
3.33. Actions/mesures temporaires prises ou prévues pour le rétablissement après l'incident	Informations précisant si l'entité financière a mis en œuvre (ou prévoit de mettre en œuvre) des mesures temporaires prises (ou prévues) pour le rétablissement après l'incident majeur lié aux TIC.	Non	Oui	Oui	Booléen (oui ou non)

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
3.34. Description de toute action et mesure temporaire prise ou prévue pour le rétablissement après l'incident	Les informations décrivent les actions immédiates prises, y compris l'isolement de l'incident au niveau du réseau, les procédures de contournement activées, les ports USB bloqués, le site de reprise après sinistre activé, tout autre contrôle de sécurité supplémentaire temporairement mis en place. Les entités financières indiquent la date et l'heure de la mise en œuvre des actions temporaires ainsi que la date prévue de retour sur le site primaire. Pour les éventuelles actions temporaires qui n'auraient pas été mises en œuvre mais qui sont encore prévues, indiquer la date à laquelle leur mise en œuvre est attendue. Si aucune action/mesure temporaire n'a été prise, veuillez en indiquer la raison.	Non	Oui, si des actions/ mesures temporaires ont été prises ou sont prévues (champ de données 3.33)	Oui, si des actions/ mesures temporaires ont été prises ou sont prévues (champ de données 3.33)	Alphanumérique
3.35. Indicateurs de compromis	Informations relatives à l'incident majeur lié aux TIC qui peuvent contribuer à la détection des activités malveillantes au sein d'un réseau ou d'un système d'information (indicateurs de compromis), le cas échéant. Ce champ ne s'applique qu'aux entités financières qui relèvent du champ d'application de la directive (UE) 2022/2555 du Parlement européen et du Conseil [1] et aux entités financières considérées comme entités essentielles ou importantes en vertu des règles nationales transposant l'article 3 de la directive (UE) 2022/2555, le cas échéant. Les indicateurs de compromis fournis par l'entité financière comprennent les catégories de données suivantes: a) les adresses IP; b) les adresses URL; c) les noms de domaine; d) les empreintes numériques; e) les données relatives aux logiciels malveillants (nom du logiciel malveillant, noms de fichiers et leur emplacement, clés de registre spécifiques associées à l'activité des logiciels malveillants); f) les données relatives à l'activité du réseau (ports, protocoles, adresses, référents, agents utilisateurs, en-têtes, journaux spécifiques ou caractéristiques distinctes du trafic réseau); g) les données du message électronique (expéditeur, destinataire, objet, en-tête, contenu);	Non	Oui, si le type d'incident «lié à la cybersécurité» est sélectionné dans le champ de données 3.23	Oui, si le type d'incident «lié à la cybersécurité» est sélectionné dans le champ de données 3.23	Alphanumérique

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
	h) les requêtes DNS et les configurations du registre; i) les activités relatives aux comptes d'utilisateur (connexions, activité de compte d'utilisateur privilégié, escalade de privilèges); j) le trafic de bases de données (lecture/écriture), les demandes dans le même fichier. Dans la pratique, ce type d'informations peut inclure des données concernant, entre autres, des indicateurs décrivant les caractéristiques du trafic réseau correspondant à des attaques connues/à des communications de réseaux zombies (botnets), les adresses IP des machines infectées par des logiciels malveillants (bots), des données relatives aux serveurs de «commande et contrôle» utilisés par des logiciels malveillants (généralement des domaines ou des adresses IP), et les URL de sites d'hameçonnage ou de sites web dont on a observé qu'ils hébergent des logiciels malveillants ou des kits d'exploit.				
Contenu du rapport final					
4.1. Classification générale des causes originelles de l'incident	Classification générale des causes originelles de l'incident majeur lié aux TIC selon les types d'incidents, y compris les catégories générales suivantes: a) actions malveillantes; b) défaillance de processus; c) défaillance/dysfonctionnement de systèmes; d) erreur humaine; e) événement extérieur.	Non	Non	Oui	Choix (plusieurs réponses possibles): — actions malveillantes, — défaillance de processus, — défaillance/dysfonctionnement de systèmes, — erreur humaine, — événement extérieur.
4.2. Classification détaillée des causes originelles de l'incident	Classification détaillée des causes originelles de l'incident majeur lié aux TIC selon les types d'incidents, y compris les catégories détaillées suivantes rattachées aux catégories générales qui sont déclarées dans le champ de données 4.1: 1. **Actions malveillantes** (si cette réponse est sélectionnée, choisissez un ou plusieurs des éléments suivants): a) actions internes délibérées; b) dommage physique délibéré/manipulation/vol; c) actions frauduleuses. 2. **Défaillance de processus** (si cette réponse est sélectionnée, choisissez un ou plusieurs des éléments suivants): a) surveillance insuffisante ou absence de surveillance et de contrôle;	Non	Non	Oui	Choix (plusieurs réponses possibles): — actions malveillantes: actions internes délibérées, — actions malveillantes: dommage physique délibéré/manipulation/vol, — actions malveillantes: actions frauduleuses, — défaillance de processus: surveillance insuffisante ou absence de surveillance et de contrôle, — défaillance de processus: rôles et responsabilités insuffisants/peu clairs, — défaillance de processus: défaillance du processus de gestion des risques liés aux TIC, — défaillance de processus: insuffisance ou défaillance des opérations de TIC et des opérations de sécurité des TIC,

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
	b) rôles et responsabilités insuffisants/peu clairs; c) défaillance du processus de gestion des risques liés aux TIC; d) insuffisance ou défaillance des opérations de TIC et des opérations de sécurité des TIC; e) gestion des projets de TIC insuffisante ou défaillante; f) politiques, procédures et documents internes inadéquats; g) acquisition, développement ou entretien inadéquats des systèmes de TIC; h) autres (veuillez préciser). 3. **Défaillance/dysfonctionnement de systèmes** (si cette réponse est sélectionnée, choisissez un ou plusieurs des éléments suivants): a) capacité et performances du matériel: incidents majeurs liés aux TIC causés par des ressources matérielles qui se révèlent inadéquates sur le plan de la capacité ou de la performance pour satisfaire aux exigences législatives applicables; b) maintenance du matériel: incidents majeurs liés aux TIC résultant d'une maintenance inadéquate ou insuffisante des composants matériels, autres que «obsolescence/vieillissement du matériel»; c) obsolescence/vieillissement du matériel: ce type de cause originelle implique des incidents majeurs liés aux TIC résultant de composants matériels obsolètes ou vieillissants; d) compatibilité/configuration des logiciels: incidents majeurs liés aux TIC causés par des composants logiciels incompatibles avec d'autres configurations de logiciels ou de systèmes, y compris les incidents majeurs liés aux TIC résultant de conflits logiciels, de paramètres incorrects ou de paramètres mal configurés qui ont une incidence sur la fonctionnalité globale du système; e) performance: incidents majeurs liés aux TIC résultant de composants logiciels peu performants ou inefficients, pour des raisons autres que celles énoncées au point «compatibilité/configuration des logiciels», y compris les incidents majeurs liés aux TIC causés par des temps de réaction lents, une consommation excessive de ressources ou une exécution inefficace des requêtes ayant une incidence sur les performances du logiciel ou du système;				— défaillance de processus: gestion des projets de TIC insuffisante ou défaillante, — défaillance de processus: inadéquation des politiques, des procédures et de la documentation internes, — défaillance de processus: acquisition, développement et entretien inadéquats des systèmes de TIC, — défaillance de processus: autres (veuillez préciser), — défaillance de systèmes: capacité et performances du matériel, — défaillance de systèmes: entretien du matériel, — défaillance de systèmes: obsolescence/vieillissement du matériel, — défaillance de systèmes: compatibilité/configuration du logiciel, — défaillance de systèmes: performance: — défaillance de systèmes: configuration du réseau, — défaillance de systèmes: dommages physiques, — défaillance de systèmes: autres (veuillez préciser), — erreur humaine: omission, — erreur humaine: erreur, — erreur humaine: compétences et connaissances, — erreur humaine: ressources humaines insuffisantes, — erreur humaine: mauvaise communication, — erreur humaine: autres (veuillez préciser), — événement extérieur: catastrophes naturelles/force majeure, — événement extérieur: défaillances de tiers, — événement extérieur: autres (veuillez préciser).

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
	f) configuration du réseau: incidents majeurs liés aux TIC résultant de paramètres ou d'infrastructures de réseau incorrects ou mal configurés, y compris les incidents majeurs liés aux TIC causés par des erreurs de configuration du réseau, des problèmes de routage, des erreurs de configuration de pare-feu ou d'autres problèmes liés au réseau perturbant la connectivité ou la communication; g) dommages physiques: incidents majeurs liés aux TIC causés par des dommages physiques aux infrastructures des TIC qui entraînent des défaillances de systèmes; h) autres (veuillez préciser). 4. **Erreur humaine** (si cette réponse est sélectionnée, choisissez un ou plusieurs des éléments suivants): a) omission (involontaire); b) erreur; c) compétences et connaissances: incidents majeurs liés aux TIC résultant d'un manque d'expertise ou de compétences dans la gestion des systèmes de TIC ou des processus de TIC, qui peut être dû à une formation inadaptée, à des connaissances insuffisantes ou à des lacunes dans les compétences requises pour accomplir des tâches particulières ou pour résoudre des problèmes techniques; d) ressources humaines insuffisantes: incidents majeurs liés aux TIC dus à l'absence des ressources nécessaires, y compris le matériel, les logiciels, les infrastructures ou le personnel, et notamment les situations dans lesquelles l'insuffisance des ressources entraîne des inefficacités opérationnelles, des défaillances de systèmes ou une incapacité à répondre aux besoins opérationnels; e) mauvaise communication; f) autres (veuillez préciser). 5. **Événement extérieur** (si cette réponse est sélectionnée, choisissez un ou plusieurs des éléments suivants): a) catastrophes naturelles/force majeure; b) défaillances de tiers;				

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
	c) autres (veuillez préciser). Les entités financières tiennent compte du fait que, pour les incidents majeurs récurrents liés aux TIC, la cause originelle apparente particulière de l'incident est prise en considération et non les grandes catégories figurant dans ce champ.				
4.3. Classification supplémentaire des causes originelles de l'incident	Classification supplémentaire des causes originelles de l'incident majeur lié aux TIC selon le type d'incident, y compris les catégories de classification supplémentaire suivantes rattachées aux catégories détaillées qui doivent être déclarées dans le champ de données 4.2. Ce champ est obligatoire pour le rapport final si des catégories particulières nécessitant une granularité plus fine sont déclarées dans le champ de données 4.2. 2.a) **Surveillance et contrôle insuffisants ou défaillants:** a) surveillance du respect des politiques; b) suivi des prestataires tiers de services; c) suivi et vérification de la correction des vulnérabilités; d) gestion des identités et des accès; e) chiffrement et cryptographie; f) journalisation. 2.c) **Défaillances du processus de gestion des risques liés aux TIC:** a) défaut de précision des niveaux exacts de tolérance au risque; b) évaluations insuffisantes des vulnérabilités et des menaces; c) inadéquation des mesures de traitement des risques; d) mauvaise gestion des risques résiduels liés aux TIC. 2.d) **Insuffisance ou défaillance des opérations de TIC et des opérations de sécurité des TIC:** a) gestion des vulnérabilités et des correctifs; b) gestion des changements; c) gestion des capacités et des performances; d) gestion des actifs de TIC et classification des informations;	Non	Non	Oui	Choix (plusieurs réponses possibles): — surveillance du respect des politiques, — suivi des prestataires tiers de services, — suivi et vérification de la correction des vulnérabilités, — gestion des identités et des accès, — chiffrement et cryptographie, — journalisation, — défaut de précision des niveaux exacts de tolérance au risque, — évaluations insuffisantes des vulnérabilités et des menaces, — inadéquation des mesures de traitement des risques, — mauvaise gestion des risques résiduels liés aux TIC, — gestion des vulnérabilités et des correctifs, — gestion des changements, — gestion des capacités et des performances, — gestion des actifs de TIC et classification des informations, — sauvegarde et restauration, — traitement des erreurs, — acquisition, développement et entretien inadéquats des systèmes de TIC, — insuffisance ou échec des essais de logiciels.

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
	e) sauvegarde et restauration; f) traitement des erreurs. 2.g) **Acquisition, développement et entretien inadéquats des systèmes de TIC:** a) acquisition, développement et entretien inadéquats des systèmes de TIC; b) insuffisance ou échec des essais de logiciels.				
4.4. Autres types de causes originelles	Les entités financières qui ont sélectionné «autres» types de causes originelles dans le champ de données 4.2 précisent ces autres types de causes originelles.	Non	Non	Oui, si «autres» types de causes originelles est sélectionné dans le champ de données 4.2	Alphanumérique
4.5. Informations sur les causes originelles de l'incident	Description de la séquence des événements qui ont conduit à l'incident majeur lié aux TIC et description de la manière dont l'incident majeur lié aux TIC a une cause originelle apparente similaire si cet incident est qualifié d'incident récurrent, y compris un exposé succinct de toutes les raisons sous-jacentes et des facteurs principaux qui ont contribué à la survenance de l'incident majeur lié aux TIC. En cas d'actions malveillantes, description du mode opératoire de l'action malveillante, y compris les tactiques, techniques et procédures utilisées, ainsi que du vecteur d'entrée de l'incident majeur lié aux TIC, y compris une description des enquêtes et des analyses qui ont permis d'identifier les causes originelles, le cas échéant.	Non	Non	Oui	Alphanumérique
4.6. Résolution de l'incident	Informations supplémentaires concernant les actions/mesures prises/prévues pour résoudre de façon définitive l'incident majeur lié aux TIC et empêcher qu'il ne se reproduise. Enseignements tirés de l'incident majeur lié aux TIC.	Non	Non	Oui	Alphanumérique

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
	La description contient les points suivants: 1. **Description des mesures de résolution** a) Actions prises pour résoudre de façon définitive l'incident majeur lié aux TIC (à l'exclusion de toute action temporaire); b) pour chaque action prise, indiquer la participation potentielle d'un prestataire tiers et de l'entité financière; c) indiquer si les procédures ont été adaptées à la suite de l'incident majeur lié aux TIC; d) indiquer tout contrôle supplémentaire qui a été mis en place ou qu'il est prévu d'instaurer, avec le calendrier de mise en œuvre correspondant. Problèmes potentiels recensés quant à la solidité des systèmes informatiques touchés ou, le cas échéant, en ce qui concerne les procédures ou contrôles en place. Les entités financières indiquent clairement la manière dont les mesures de réparation envisagées traiteront les causes originelles identifiées et la date à laquelle elles comptent sur la résolution définitive de l'incident majeur lié aux TIC. 2. **Enseignements tirés** Les entités financières décrivent les conclusions de l'examen post-incident.				
4.7. Date et heure de traitement de la cause originelle de l'incident	Date et heure de traitement de la cause originelle de l'incident.	Non	Non	Oui	Norme ISO 8601 TUC (aaaa-mm-jj hh: mm:ss)
4.8. Date et heure de résolution de l'incident	Date et heure de résolution de l'incident.	Non	Non	Oui	Norme ISO 8601 TUC (aaaa-mm-jj hh: mm:ss)

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
4.9. Informations précisant si la date de résolution définitive des incidents diffère de la date de mise en œuvre initialement prévue	Description de la raison pour laquelle la date de résolution définitive des incidents majeurs liés aux TIC diffère de la date de mise en œuvre initialement prévue, le cas échéant.	Non	Non	Oui	Alphanumérique
4.10. Évaluation des risques pour les fonctions critiques aux fins de la résolution	Évaluation visant à déterminer si l'incident majeur lié aux TIC présente un risque pour les fonctions critiques au sens de l'article 2, paragraphe 1, point 35), de la directive 2014/59/UE du Parlement européen et du Conseil ([2]). Les entités visées à l'article 1er, paragraphe 1, de la directive 2014/59/UE indiquent si l'incident présente un risque pour les fonctions critiques au sens de l'article 2, paragraphe 1, point 35), de ladite directive, déclarées dans le modèle Z 07.01 du règlement d'exécution (UE) 2018/1624 de la Commission ([3]) et mises en correspondance avec l'entité spécifique dans le modèle Z 07.02.	Non	Non	Oui, si l'incident présente un risque pour les fonctions critiques d'entités financières au sens de l'article 2, paragraphe 1, point 35), de la directive 2014/59/UE	Alphanumérique
4.11. Informations utiles aux autorités de résolution	Description indiquant si l'incident majeur lié aux TIC a compromis la résolvabilité de l'entité ou du groupe et, dans l'affirmative, la manière dont il l'a compromise. Les entités visées à l'article 1er, paragraphe 1, de la directive 2014/59/UE indiquent si l'incident majeur lié aux TIC a compromis la résolvabilité de l'entité ou du groupe et, dans l'affirmative, la manière dont il l'a compromise. Ces entités indiquent également si l'incident majeur lié aux TIC nuit à la solvabilité ou à la liquidité de l'entité financière et à la quantification potentielle de l'incidence. Ces entités fournissent également des informations relatives à l'incidence sur la continuité opérationnelle, à l'incidence sur la résolvabilité de l'entité, à toute incidence supplémentaire sur les coûts et les pertes dus à l'incident majeur lié aux TIC, y compris sur la situation des fonds propres de l'entité financière, et elles indiquent si les accords contractuels relatifs à l'utilisation de services TIC sont toujours solides et pleinement exécutoires en cas de résolution de l'entité.	Non	Non	Oui, si l'incident a compromis la résolvabilité de l'entité ou du groupe	Alphanumérique

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
4.12. Seuil d'importance significative pour le critère de classification «conséquences économiques»	Informations détaillées sur les seuils finalement atteints par l'incident majeur lié aux TIC en ce qui concerne le critère «conséquences économiques» prévu aux articles 7 et 14 du règlement délégué (UE) 2024/1772.	Non	Non	Oui	Alphanumérique
4.13. Montant des coûts et pertes directs et indirects bruts	Montant total des coûts et pertes directs et indirects bruts supportés par l'entité financière en raison de l'incident majeur lié aux TIC, englobant: a) le montant des fonds ou des actifs financiers expropriés dont l'entité financière est responsable; b) le montant des coûts du remplacement ou du déplacement de logiciels, de matériel ou d'infrastructures; c) le montant des frais de personnel, y compris les coûts liés au remplacement ou au déménagement du personnel, au recrutement de personnel supplémentaire, à la rémunération des heures supplémentaires et à la récupération des compétences perdues ou altérées; d) le montant des frais dus au non-respect d'obligations contractuelles; e) le montant des coûts de dédommagement et d'indemnisation des clients; f) le montant des pertes dues aux recettes non perçues; g) le montant des coûts liés à la communication interne et externe; h) le montant des frais de conseil, y compris les coûts liés au conseil juridique, aux services d'analyse forensique et aux services de remédiation; i) le montant des autres coûts et pertes, y compris: i) les charges directes portées au compte de résultat, dépréciations et frais de règlement compris, et les réductions de valeur dues à l'incident majeur lié aux TIC; ii) les provisions ou réserves inscrites au compte de résultat pour pertes probables liées à l'incident majeur lié aux TIC;	Non	Non	Oui	Monétaire

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
	iii) les pertes latentes, à savoir les pertes dues à l'incident majeur lié aux TIC qui sont temporairement inscrites dans des comptes transitoires ou d'attente et ne sont donc pas encore portées au compte de résultat et qu'il est prévu d'inclure dans un délai correspondant à la taille et à l'âge du poste en suspens; iv) les recettes non perçues d'un montant significatif liées à des obligations contractuelles envers des tiers, y compris à la décision, consécutive à l'incident majeur lié aux TIC, d'indemniser un client non par remboursement ou paiement direct, mais par un ajustement des recettes consistant à ne pas appliquer, ou à réduire, des frais contractuels sur une certaine période à venir; v) les pertes temporaires, lorsqu'elles couvrent plus d'un exercice financier et s'accompagnent d'un risque juridique. Les entités financières tiennent compte, dans leur évaluation, de l'article 7, paragraphes 1 et 2, du règlement délégué (UE) 2024/1772. Elles n'incluent dans ce chiffre aucun recouvrement financier de quelque nature que ce soit. Les entités financières déclarent le montant monétaire comme une valeur positive. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, les entités financières tiennent compte du montant total des coûts et pertes pour toutes les entités financières. Les entités financières déclarent le point de données en unités avec une précision minimale fixée au millier d'unités.				
4.14. Montant des recouvrements financiers	Montant total des recouvrements financiers. Les recouvrements financiers se rapportent à la perte initiale causée par l'incident, quel que soit le moment où les recouvrements financiers sous la forme de fonds ou de flux d'avantages économiques sont reçus.	Non	Non	Oui	Monétaire Les entités financières déclarent le point de données en unités avec une précision minimale fixée au millier d'unités.

Champ de données	Description	Obligatoire pour la notification initiale	Obligatoire pour le rapport intermédiaire	Obligatoire pour le rapport final	Type de champ
	Les entités financières déclarent le montant monétaire comme une valeur positive. En cas de déclaration agrégée prévue à l'article 7 du présent règlement, les entités financières tiennent compte du montant total des recouvrements financiers dans toutes les entités financières.				
4.15. Informations précisant si les incidents non majeurs ont été récurrents	Informations précisant si plusieurs incidents non majeurs liés aux TIC ont été récurrents et s'ils sont considérés ensemble comme un incident majeur au sens de l'article 8, paragraphe 2, du règlement délégué (UE) 2024/1772. Les entités financières indiquent si les incidents non majeurs liés aux TIC ont été récurrents et s'ils sont considérés ensemble comme un incident majeur lié aux TIC. Les entités financières indiquent également le nombre de ces incidents non majeurs liés aux TIC.	Non	Non	Oui, si l'incident majeur comprend plusieurs incidents récurrents non majeurs	Alphanumérique
4.16. Date et heure auxquelles les incidents récurrents sont survenus	Lorsque les entités financières déclarent des incidents récurrents liés aux TIC, elles indiquent la date et l'heure auxquelles le premier incident lié aux TIC est survenu.	Non	Non	Oui, pour les incidents récurrents	Norme ISO 8601 TUC (aaaa-mm-jj hh: mm:ss)

(1) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(2) Directive 2014/59/UE du Parlement européen et du Conseil du 15 mai 2014 établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement et modifiant la directive 82/891/CEE du Conseil ainsi que les directives du Parlement européen et du Conseil 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE et 2013/36/UE et les règlements du Parlement européen et du Conseil (UE) nº 1093/2010 et (UE) nº 648/2012 (JO L 173 du 12.6.2014, p. 190, ELI: http://data.europa.eu/eli/dir/2014/59/oj).

(3) Règlement d'exécution (UE) 2018/1624 de la Commission du 23 octobre 2018 définissant des normes techniques d'exécution concernant les procédures, les formulaires types et les modèles à utiliser pour la fourniture d'informations aux fins de l'établissement de plans de résolution pour les établissements de crédit et les entreprises d'investissement, conformément à la directive 2014/59/UE du Parlement européen et du Conseil, et abrogeant le règlement d'exécution (UE) 2016/1066 de la Commission (JO L 277 du 7.11.2018, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2018/1624/oj).

ANNEXE III

MODÈLES DE NOTIFICATION DES CYBERMENACES IMPORTANTES

Numéro du champ	Champ de données	
1	Nom de l'entité soumettant la notification	
2	Code d'identification de l'entité soumettant la notification	
3	Type de l'entité financière soumettant la notification	
4	Nom de l'entité financière	
5	Code LEI de l'entité financière	
6	Nom de la personne de contact principale	
7	Adresse électronique de la personne de contact principale	
8	Numéro de téléphone de la personne de contact principale	
9	Nom de la deuxième personne de contact	
10	Adresse électronique de la deuxième personne de contact	
11	Numéro de téléphone de la deuxième personne de contact	
12	Date et heure de détection de la cybermenace	
13	Description de la cybermenace importante	
14	Informations relatives à l'incidence potentielle	
15	Critères de classification de l'incident potentiel	
16	Situation de la cybermenace	
17	Actions prises pour empêcher la matérialisation	
18	Notification aux autres parties prenantes	
19	Indicateurs de compromis	
20	Autres informations utiles	

ANNEXE IV

GLOSSAIRE DE DONNÉES ET INSTRUCTIONS POUR LA NOTIFICATION DES CYBERMENACES IMPORTANTES

Champ de données	Description	Champ obligatoire	Type de champ
1. Nom de l'entité soumettant la notification	Dénomination sociale complète de l'entité soumettant la notification.	Oui	Alphanumérique
2. Code d'identification de l'entité soumettant la notification	Code d'identification de l'entité soumettant la notification. Lorsque les entités financières soumettent la notification/le rapport, le code d'identification est l'identifiant d'entité juridique (LEI), code unique à 20 caractères alphanumériques conforme à la norme ISO 17442-1:2020. Lorsqu'un prestataire tiers soumet un rapport au nom d'une entité financière, il peut utiliser un code d'identification tel que spécifié dans les normes techniques d'exécution adoptées en vertu de l'article 28, paragraphe 9, du règlement (UE) 2022/2554.	Oui	Alphanumérique
3. Type d'entité financière soumettant le rapport	Type de l'entité, tel qu'énuméré à l'article 2, paragraphe 1, points a) à t), du règlement (UE) 2022/2554, qui soumet le rapport.	Oui, si le rapport n'est pas transmis directement par l'entité financière touchée	Choix (sélection multiple): — les établissements de crédit, — les établissements de paiement, — les établissements de paiement exemptés, — les prestataires de services d'information sur les comptes, — les établissements de monnaie électronique, — les établissements de monnaie électronique exemptés, — les entreprises d'investissement, — les prestataires de services sur crypto-actifs, — les émetteurs de jetons se référant à un ou des actifs, — les dépositaires centraux de titres, — les contreparties centrales, — les plates-formes de négociation, — les référentiels centraux, — les gestionnaires de fonds d'investissement alternatifs, — les sociétés de gestion, — les prestataires de services de communication de données,

Champ de données		Description	Champ obligatoire	Type de champ
				— les entreprises d'assurance et de réassurance, — les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire, — les institutions de retraite professionnelle, — les agences de notation de crédit, — les administrateurs d'indices de référence d'importance critique, — les prestataires de services de financement participatif, — les référentiels des titrisations.
4.	Nom de l'entité financière	Dénomination sociale complète de l'entité financière notifiant la cybermenace importante.	Oui, si l'entité financière diffère de l'entité qui soumet la notification	Alphanumérique
5.	Code LEI de l'entité financière	Identifiant d'entité juridique (LEI) de l'entité financière notifiant la cybermenace importante, attribué conformément aux normes établies par l'Organisation internationale de normalisation.	Oui, si l'entité financière notifiant la cybermenace importante diffère de l'entité qui soumet le rapport	Code unique à 20 caractères alphanumériques, conforme à la norme ISO 17442-1:2020
6.	Nom de la personne de contact principale	Nom et prénom de la personne de contact principale de l'entité financière.	Oui	Alphanumérique
7.	Adresse électronique de la personne de contact principale	Adresse électronique de la personne de contact principale que l'autorité compétente peut utiliser pour la communication de suivi.	Oui	Alphanumérique
8.	Numéro de téléphone de la personne de contact principale	Numéro de téléphone de la personne de contact principale que l'autorité compétente peut utiliser pour la communication de suivi. Le numéro de téléphone indiqué comporte tous les préfixes internationaux (par exemple +33 XXXXXXXXX).	Oui	Alphanumérique
9.	Nom de la deuxième personne de contact	Nom et prénom de la deuxième personne de contact de l'entité financière ou, lorsqu'ils sont disponibles, de l'entité qui soumet la notification au nom de l'entité financière.	Oui, si les nom et prénom de la deuxième personne de contact de l'entité financière ou de l'entité qui soumet la notification pour l'entité financière sont disponibles	Alphanumérique

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Champ de données	Description	Champ obligatoire	Type de champ
10. Adresse électronique de la deuxième personne de contact	Adresse électronique de la deuxième personne de contact ou adresse électronique fonctionnelle de l'équipe que l'autorité compétente peut utiliser pour la communication de suivi, le cas échéant.	Oui, si l'adresse électronique de la deuxième personne de contact ou une adresse électronique fonctionnelle de l'équipe que l'autorité compétente peut utiliser pour la communication de suivi est disponible	Alphanumérique
11. Numéro de téléphone de la deuxième personne de contact	Numéro de téléphone de la deuxième personne de contact que l'autorité compétente peut utiliser pour la communication de suivi, le cas échéant. Le numéro de téléphone indiqué comporte tous les préfixes internationaux (par exemple +33 XXXXXXXXX).	Oui, si le numéro de téléphone de la deuxième personne de contact que l'autorité compétente peut utiliser pour la communication de suivi est disponible	Alphanumérique
12. Date et heure de détection de la cybermenace	Date et heure auxquelles l'entité financière a pris connaissance de la cybermenace importante.	Oui	Norme ISO 8601 TUC (aaaa-mm-jj hh:mm:ss)
13. Description de la cybermenace importante	Description des aspects les plus pertinents de la cybermenace importante. Les entités financières présentent: a) un aperçu schématique des aspects les plus pertinents de la cybermenace importante; b) les risques connexes qui en découlent, y compris les vulnérabilités potentielles des systèmes de l'entité financière qui peuvent être exploitées; c) des informations sur la probabilité de matérialisation de la cybermenace importante; et d) des informations concernant la source d'informations sur la cybermenace.	Oui	Alphanumérique
14. Informations relatives à l'incidence potentielle	Informations relatives à l'incidence potentielle de la cybermenace, en cas de matérialisation, sur l'entité financière, ses clients ou ses contreparties financières.	Oui	Alphanumérique
15. Critères de classification de l'incident potentiel	Les critères de classification qui auraient pu donner lieu à une déclaration d'incident majeur si la cybermenace s'était matérialisée.	Oui	Choix (plusieurs réponses possibles): — clients, contreparties financières et transactions touchés, — atteinte à la réputation, — durée et interruptions de service, — répartition géographique, — pertes de données, — services critiques touchés, — conséquences économiques.

Champ de données		Description	Champ obligatoire	Type de champ
16.	Situation de la cybermenace	Informations sur la situation de la cybermenace pour l'entité financière et sur l'évolution éventuelle de l'activité de la menace. Lorsque la cybermenace a cessé de communiquer avec les systèmes d'information de l'entité financière, elle peut être qualifiée d'inactive. Si l'entité financière dispose d'informations indiquant que la menace demeure active à l'égard d'autres parties ou du système financier dans son ensemble, la menace est qualifiée d'active.	Oui	Choix: — active, — inactive.
17.	Mesures prises pour empêcher la matérialisation	Informations générales sur les actions prises par l'entité financière pour empêcher la matérialisation des cybermenaces importantes, le cas échéant.	Oui	Alphanumérique
18.	Notification aux autres parties prenantes	Informations sur la notification de la cybermenace à d'autres entités ou autorités financières.	Oui, si d'autres entités ou autorités financières ont été informées de la cybermenace	Alphanumérique
19.	Indicateurs de compromis	Informations relatives à la menace importante qui peuvent contribuer à la détection des activités malveillantes au sein d'un réseau ou d'un système d'information (indicateurs de compromis), le cas échéant. Les indicateurs de compromis fournis par l'entité financière peuvent inclure, sans s'y limiter, les catégories de données suivantes: a) les adresses IP; b) les adresses URL; c) les noms de domaine; d) les empreintes numériques; e) les données relatives aux logiciels malveillants (nom du logiciel malveillant, noms de fichiers et leur emplacement, clés de registre spécifiques associées à l'activité des logiciels malveillants); f) les données relatives à l'activité du réseau (ports, protocoles, adresses, référents, agents utilisateurs, en-têtes, journaux spécifiques ou caractéristiques distinctes du trafic réseau); g) les données du message électronique (expéditeur, destinataire, objet, en-tête, contenu); h) les requêtes DNS et les configurations du registre; i) les activités relatives aux comptes d'utilisateur (connexions, activité de compte d'utilisateur privilégié, escalade de privilèges); j) le trafic de bases de données (lecture/écriture), les demandes dans le même fichier. Ce type d'informations peut inclure des données concernant des indicateurs décrivant les caractéristiques du trafic réseau correspondant à des attaques connues/à des communications de réseaux zombies (botnets), les adresses IP des machines infectées par des logiciels malveillants (bots), des données relatives aux serveurs de «commande et contrôle» utilisés par des logiciels malveillants (généralement des domaines ou des adresses IP) et les URL de sites d'hameçonnage ou de sites web dont on a observé qu'ils hébergent des logiciels malveillants ou des kits d'exploit.	Oui, si des informations relatives à des indicateurs de compromis en rapport avec la cybermenace sont disponibles	Alphanumérique
20.	Autres informations utiles	Toute autre information utile concernant la cybermenace importante	Oui, s'il y a lieu et si d'autres informations, non reprises dans le modèle, sont disponibles	Alphanumérique