regulation partners

Regulation Partners

Les rendez vous de la régulation

Conférence AEFR

Le rendez-vous de l’actualité sur la régulation LCB-FT, DORA et l’IA

Jeudi 19 Juin 2025

AMLD 6 et Règlement (UE) 2024/1624 du Parlement européen et du Conseil du 31 mai 2024

- **AMLD 6 :** Entrée en vigueur le 9 juillet 2024
- Applicable à partir du 10 juillet 2027 pour une grande partie
- Registre des comptes bancaires étendu aux informations sur les crypto actifs, comptes titres, comptes de paiement et coffres.
- La directive prévoit que ces registres automatisés centralisés soient interconnectés à l'échelle de l'UE afin de permettre aux CRF d'obtenir rapidement les informations transfrontières sur les détenteurs des comptes ainsi renseignés.
- ajout au registre des comptes bancaires des IBAN virtuels, assorti d'une obligation, pour les émetteurs de ces IBAN, d'identifier leurs utilisateurs.

AMLR : entrée en vigueur le 10/07/2024

- Sera d'application au 10/07/2027
- étend le champ des entités supervisées :

Notamment tous les prestataires de services sur crypto-actifs (PSCA) tels que définis par le règlement MiCA, à l'exception des services de conseil sur cryptoactifs (possibilité pour les États membres de les superviser s'ils le souhaitent)

Dispositions clés du règlement : Renforcement des mesures de vigilance

Transactions à titre occasionnel

identifier / vérifier l'identité de leur client avant l'exécution d'une transaction à titre occasionnel.

En France, cela s'impose à ce jour, qu'en cas de soupçon de BC-FT, lorsque l'opération excède certains seuils fixés par l'article R.561-10 du code monétaire et financier ou lorsque l'opération concernée est une transmission de fonds ou un transfert effectué auprès d'un prestataire de services sur crypto-actifs.

Renforcement des mesures de vigilance mise en œuvre par les entités supervisées

Extension des informations à collecter sur les clients selon qu'il s'agit d'une PP, PM, d'un trust ou d'une fiducie, mesures de vigilance renforcées :

- Devront être appliquées pour toutes les transactions, y compris occasionnelles, impliquant un pays tiers à haut risque selon les listes établies par le Groupe d'action financière (GAFI)
- Limite maximale de 10 000 euros fixée pour les paiements en espèces à l'échelle de l'UE (Article 80)

Nouveau régime concernant les PPE

- Par rapport au cadre actuel , la liste des fonctions PE est élargie aux chefs des exécutifs des collectivités locales (régions, départements, communes et intercommunalités d'au moins 50 000 habitants) ainsi qu'aux membres des organes d'administration, de direction ou de surveillance des entreprises publiques locales à partir de 8 millions d'euros de chiffre d'affaires (Article 2- paragraphe 34)
- AMLR précise la notion de conjoint et étend les mesures applicables aux PPE aux frères et sœurs des chefs d'État, chefs de gouvernement, ministres, ministres délégués et secrétaires d'État ou aux personnes exerçant des fonctions équivalentes au niveau de l'UE ou dans un pays tiers.
- Alors que le cadre actuel prévoit la mise en œuvre des mesures spécifiques aux PPE aux seules relations d'affaires, AMLR les étend à toute transaction ou activité menée pour le compte ou au profit d'une PPE, d'un membre de sa famille ou d'une personne connue pour lui être étroitement associées.

Mesures de vigilance concernant les transactions en crypto-actifs

- Les PSCA devront appliquer les mesures de vigilance à l'égard de leur clientèle pour toutes les transactions réalisées à titre occasionnel supérieures ou égales à 1000 euros (Article 19)
- Des mesures de vigilance renforcées sont prévues pour les relations transfrontalières de correspondant entre PSCA.
- Des mesures de vigilance renforcée sont prévues pour les transactions depuis ou vers des portefeuilles de crypto-actifs auto-hébergés.

Dispositions clés du règlement : Précision des dispositions concernant l'identification du bénéficiaire effectif

- Pour l'identification du ou des bénéficiaires effectifs, la définition reste inchangée tout comme le seuil permettant de déterminer la participation au capital d'une entreprise, fixé à 25 % ou plus des actions, droits de vote ou autres participations au capital de l'entreprise, y compris les droits à une part des bénéfices, d'autres ressources internes ou le solde de liquidation.
- Il est toutefois précisé que toutes les participations, quel que soit leur niveau de propriété, doivent être prises en considération.
- De plus, en adoptant une approche fondée sur les risques, les États membres peuvent recenser les catégories d'entreprises exposées à des risques BC-FT plus élevés et proposer à la Commission un seuil plus bas ; ce dernier ne pouvant toutefois pas être inférieur à 15 %.
- Des registres doivent être tenus afin de consigner les mesures prises pour identifier le bénéficiaire effectif.
- Le registre des bénéficiaires effectifs doit être complété des informations sur les bénéficiaires effectifs des entités juridiques étrangères situées hors de l'UE lorsqu'elles entrent en relation d'affaires avec des professions supervisées situées dans l'UE, achètent un bien immobilier dans l'UE ou obtiennent un marché public dans l'UE.
- Des informations sur l'historique des bénéficiaires effectifs des cinq dernières années et la description de la structure de détention ou de contrôle des personnes morales sont également requises.

- Dans le cas où aucun bénéficiaire effectif n'a pu être déterminé, une déclaration doit l'accompagner, justifiant pourquoi aucune identification n'a été possible.
- De plus, des exigences plus strictes ont été prévues pour la déclaration des divergences par rapport aux informations contenues dans les registres des bénéficiaires effectifs.
- Les entités supervisées doivent déclarer toute divergence constatée entre les informations disponibles dans le registre des bénéficiaires effectifs et les informations qu'elles sont tenues de recueillir.
- Les divergences sont signalées à l'entité chargée de la gestion du registre dans les meilleurs délais et, en tout état de cause, dans les quatorze jours calendaires suivant leur détection.
- Lorsqu'elles signalent de telles divergences, les entités supervisées joignent à leur rapport les informations qu'elles ont obtenues, en décrivant la divergence et les personnes qu'elles considèrent comme les bénéficiaires effectifs et, le cas échéant, les actionnaires apparents et les administrateurs apparents.

Focus sur le Règlement (UE) 2024/1624 du Parlement européen et du Conseil du 31 mai 2024

regulation partners

Comparaison des listes de PPE : Arrêté du 17 mars 2023 vs Règlement européen 2024/1624

Catégorie de PPE	Arrêté du 17 mars 2023	Règlement européen 2024/1624	Comparaison
Chefs de l'Exécutif	Président de la République Premier ministre Membres du Gouvernement	Chefs d'État, chefs de gouvernement, ministres, ministres délégués et secrétaires d'État (dans un État membre, à l'Union, ou dans un pays tiers)	Le règlement européen inclut explicitement les secrétaires d'État.
Législateurs	Président du Sénat Président de l'Assemblée nationale Députés et sénateurs	Parlementaires ou membres d'organes législatifs similaires (dans un État membre, à l'Union, ou dans un pays tiers)	
Partis politiques	Présidents et membres des organes exécutifs des partis ou groupements politiques soumis à la loi n° 88-27 du 11 mars 1988 ou personnes exerçant des fonctions équivalentes.	Membres des organes dirigeants des partis politiques qui occupent des sièges dans des organes exécutifs ou législatifs nationaux, ou dans des organes exécutifs ou législatifs régionaux ou locaux représentant des circonscriptions d'au moins 50 000 habitants.	Le règlement européen apporte une précision en incluant les partis politiques au niveau régional et local, avec un seuil de population.
Fonctions juridictionnelles / Hautes juridictions Et instances de supervision	Président et membres du Conseil constitutionnel (ainsi que le secrétaire général), Membres du Conseil d'État & Magistrats de la Cour des comptes & Membres de la Cour de cassation, membres du conseil général de la banque de France Les ambassadeurs ou chargés d'affaires, Le chef d'état-major	Membres des cours suprêmes, des cours constitutionnelles ou d'autres hautes juridictions dont les décisions ne sont pas susceptibles de recours, sauf circonstances exceptionnelles Membres des cours des comptes ou des conseils ou directoires des banques centrales les ambassadeurs, les chargés d'affaires et les officiers supérieurs des forces armées, autres personnes exerçant des fonctions publiques importantes prévues par les États membres	Le règlement européen généralise en citant les fonctions juridictionnelles suprêmes ou constitutionnelles, et ajoute les responsables des collectivités régionales et locales sous critère d'un seuil de population. Le règlement stipule que les fonctions publiques importantes prévues par les États membres non citées dans le présent règlement sont considérées PPE

Catégorie de PPE	Arrêté du 17 mars 2023	Règlement européen 2024/1624	Comparaison
Dirigeants d'Entreprises publiques / contrôlées et dirigeants des collectivités…	Dirigeants (DG, administrateurs, etc.) de sociétés, établissements publics, etc. mentionnés aux 1°, 3° et 5° du III de l'article 11 de la loi du 11 octobre 2013- Pour le 5° (certaines personnes morales), un chiffre d'affaires annuel > 50 millions d'euros est requis.	Membres des organes d'administration, de direction ou de surveillance des entreprises contrôlées par l'État, ou (pour les moyennes/grandes entreprises/groupes) par des autorités régionales ou locales. les responsables des collectivités régionales et locales, y compris des regroupements de communes et des régions métropolitaines d'au moins 50 000 habitants	
Organisations internationales et UE	Non concerné (décret national)	Hauts responsables et membres du conseil d'organisations internationales ou personnes équivalentes Représentants auprès d'un État membre ou de l'Union.	Le règlement européen a une portée plus large, reconnaissant les risques associés aux fonctions exercées au sein des organisations internationales et des institutions de l'UE.

Synthèse des travaux de l'ABE sur ses projets de standards techniques réglementaires (RTS) dans le cadre du futur dispositif européen de LCB-FT

Contexte

Consultation publique de l'ABE le 6 mars 2025 sur :

- 4 projets de standards techniques réglementaire
- feront partie de sa réponse à l'appel à avis de la Commission européenne du 12 mars 2024.
- Cet appel porte sur la préparation de 4 mandats réglementaires

• l'article 40(2) de la directive (UE) 2024/1640, visant à élaborer un projet de RTS relatif à l'évaluation et à la classification du profil de risque intrinsèque et résiduel des entités assujetties, ainsi qu'à la fréquence de révision de ce profil.
• l'article 12(7) du règlement (UE) 2024/1620 (AMLAR), visant à élaborer un projet de RTS relatif à l'évaluation des risques aux fins de sélection en vue d'un contrôle direct.
• l'article 28(1) du règlement (UE) 2024/1624 (AMLR), visant à élaborer un projet de RTS relatif à la vigilance à l'égard de la clientèle (Customer Due Diligence - CDD).
• l'article 53(10) de la sixième directive anti-blanchiment (AMLD6), visant à élaborer un projet de RTS relatif aux sanctions pécuniaires, aux mesures administratives et aux astreintes.

« Ces projets et les contributions reçues dans le cadre de la consultation auront vocation à alimenter les travaux de la nouvelle autorité de lutte contre le blanchiment de capitaux et le financement du terrorisme (*AMLA*), qui sera formellement chargée d'élaborer ces RTS et de les soumettre à la Commission pour approbation. La consultation est ouverte jusqu'au 6 juin 2025. » source : https://www.amf-france.org/fr/actualites-publications/actualites/lamf-invite-les-acteurs-de-la-place-repondre-la-consultation-de-leba-sur-des-projets-de-normes.

La Commission européenne a demandé à l'ABE d'élaborer les normes techniques susmentionnées afin de soutenir le démarrage rapide et efficace des opérations de lutte contre le blanchiment de capitaux. L'ABE soumettra sa réponse, assortie de ces normes techniques, à la Commission européenne le 31 octobre 2025.

Détails du RTS N°1

RTS sur la méthodologie d'évaluation du profil de risque inhérent et résiduel des entités assujetties et fréquence à laquelle ce profil doit être revu

Référence : Article 40(2) de la Directive (UE) 2024/1640 – AMLD6

Objectif :
L'article 40(2) requiert une évaluation du profil de risque intrinsèque et résiduel. Ce RTS objective la manière d'évaluer les risques inhérents de BC/FT associé à chaque établissement via une méthodologie harmonisée que tous les superviseurs nationaux appliqueront, permettant également de déterminer la qualité des contrôles et les risques résiduels qui subsistent après leur mise en œuvre.
L'approche proposée garantira que les évaluations des risques au niveau des entités par les superviseurs sont cohérentes avec des résultats comparables entre les États membres. Elle réduirait également la charge réglementaire pour les établissements transfrontaliers, notamment grâce à l'harmonisation des demandes d'informations des différents superviseurs.

Définition des termes (article 1) :

« Risque intrinsèque » : risque qu'une entité puisse être utilisée à des fins de BC/FT, compte tenu du degré auquel les produits, services et types de transactions qu'elle propose, la clientèle qu'elle dessert, les juridictions dans lesquelles elle opère et les canaux de distribution qu'elle utilise affectent la traçabilité des fonds, l'identité du bénéficiaire effectif final et la facilité à vérifier la légitimité de l'activité des clients

« Risque résiduel » : risque qu'une entité puisse être utilisée à des fins de BC/FT, compte tenu des risques intrinsèques auxquels elle est exposée et de la qualité des procédures, systèmes et contrôles LCB/FT mis en place par l'entité assujettie pour atténuer ces risques

« Pondération » : ensemble d'indicateurs, de sous-catégories ou de catégories d'indicateurs servant à établir un score combiné, le degré d'influence de chacun de ces éléments sur la détermination du score final. Les indicateurs, sous-catégories et catégories ayant une pondération plus faible auront une influence moindre que ceux ayant une pondération plus élevée.

AMLD6 + RTS Article 40

- Méthodologie harmonisée obligatoire dans toute l'UE
- Automatisation par indicateurs chiffrés, avec ajustements encadrés
- Barèmes standardisés et comparables entre superviseurs
- Périodicité obligatoire (annuelle ou triennale)
- Introduction de données sectorielles détaillées

Détails du RTS N°1

Contenu du RTS :

(articles 2 à 4) Évaluation en 3 étapes :

- **Évaluer/classifier les risque intrinsèque** à l'aide d'indicateurs reflétant le niveau d'exposition au BC/FT (les risques intrinsèques viennent de différents facteurs tels que la nature du client, le type de produit, la zone géographique d'activité etc.)
- **Évaluer la qualité des contrôles internes LCB-FT mis en place par l'entité**
- **Évaluer le profil de risque résiduel** (combinaison des 2 scores précédents, soit le risque restant après application des mesures de contrôle)

(articles 2 à 4) Échelle commune de classification pour les 3 étapes :

- **1 (Faible) à 4 (Élevé) pour les risques**
- **A (Très bon) à D (Mauvais) pour les contrôles**

(article 5) 1ère revue au plus tard dans un délai de 9 mois suivant la date d'entrée en vigueur du règlement, puis revue annuelle obligatoire (avant le 30 sept), sauf :

- **Triennale pour les entités :**
  - ≤ 5 salariés
  - N'exercent pas d'activité relevant du règlement (UE) 2024/1624, **sauf les activités citées en détail de l'article 5 - b du présent RTS**
  - L'entité est une succursale établie par un organisme de placement collectif au sens de l'art. 2, §1, point 6(e) du règlement (UE) 2024/1624, et autorisée dans un autre État membre
  - Son profil de risque résiduel a déjà été évalué au moins une fois conformément à l'article 5 et classé dans la catégorie risque faible
- **Revue ad hoc si événements significatifs dans un délai de 4 mois à compter du moment où elles en ont connaissance**

(Article 6) Entrée en vigueur :

Le règlement entre en vigueur le 20e jour suivant celui de sa publication au Journal officiel de l'Union européenne (obligatoire dans tous ses éléments et directement applicable dans tous les États membres).

Évaluation et classification du profil de risque intrinsèque des entités assujetties (Indicateurs en Annexe I Section A) :

Sur la base du score déterminé (ajusté ou non), l'entité est classée selon le barème suivant :

- **Score < 1,75** : Risque faible (1)
- **1,75 ≤ Score < 2,5** : Risque moyen (2)
- **2,5 ≤ Score < 3,25** : Risque substantiel (3)
- **Score ≥ 3,25** : Risque élevé (4)

Évaluation et classification de la qualité des contrôles LCB/FT mis en place par les entités assujetties (Indicateurs en Annexe I Section B) :

Sur la base de ce score, l'entité est classée comme suit :

Score < 1,75 : Très bonne qualité des contrôles (A)
1,75 ≤ Score < 2,5 : Bonne qualité des contrôles (B)
2,5 ≤ Score < 3,25 : Qualité moyenne des contrôles (C)
Score ≥ 3,25 : Mauvaise qualité des contrôles (D)

Évaluation et classification du profil de risque résiduel des entités assujetties (combinaison des 2 premiers indicateurs)

Sur la base du score de risque résiduel obtenu, les autorités classent l'entité selon les seuils suivants :

Score < 1,75 : Risque faible (1)
1,75 ≤ Score < 2,5 : Risque moyen (2)
2,5 ≤ Score < 3,25 : Risque substantiel (3)
Score ≥ 3,25 : Risque élevé (4)

Détails du RTS N°2

regulation partners

RTS sur l'évaluation des risques aux fins de la sélection des entités soumises à la surveillance directe de l'AMLA

Référence : Article 12(7) du Règlement (UE) 2024/1620 – AMLAR

Objectif :
Ce RTS se concentre sur La manière dont la nouvelle Autorité européenne de lutte contre le blanchiment de capitaux et le financement du terrorisme (AMLA) décidera des institutions soumises à la surveillance directe. L'ABE propose que l'AMLA détermine d'abord les institutions éligibles à la surveillance directe en tenant compte de leurs activités transfrontalières. Dans un second temps, l'AMLA examinerait les résultats de la méthodologie harmonisée d'évaluation des risques de blanchiment de capitaux et de financement du terrorisme (BC/FT).

Contenu du RTS :

• (Article 1) Critères géographiques :
- Activité dans au moins 6 États membres (établissement ou services transfrontaliers)
- Prestation de services prise en compte si :
  - ≥ 20 000 clients *ou*
  - ≥ 50 M€ de volume de transactions.
  - (Le respect de ces seuils est évalué à partir de l'annexe I Section C)

• (Article 2 à 4) Méthodologie de scoring :
- identique à celle des 3 étapes du 1er RTS traité

• (article 5) Score de groupe :
- Moyenne pondérée des scores de chaque entité du groupe, avec pondération plus forte pour les entités à haut risque ou importantes en taille (voir détail slide N°7)

• (article 6) Clause transitoire :
- pour le 1er cycle d'évaluation, les superviseurs ne peuvent ajuster les scores de contrôle (article 3.3 ne s'applique pas) manuellement de ±1 par catégorie sauf cas exceptionnels (à voir dans le détail du RTS)

• (article 7) Entrée en vigueur :
Le règlement entre en vigueur le 20e jour suivant celui de sa publication au Journal officiel de l'Union européenne (obligatoire dans tous ses éléments et directement applicable dans tous les États membres).

AMLAR + RTS Article 12

- Introduction d'une supervision directe européenne par l'AMLA
- Seuils précis (clients, volumes) pour identifier les entités à enjeu européen
- L'AMLA peut s'imposer directement sur certaines entités
- Score harmonisé à l'échelle du groupe et à l'échelle de l'UE

Détails du RTS N°2

Évaluation et classification du profil de risque intrinsèque des entités assujetties (Indicateurs en Annexe I Section A) :

Sur la base du score déterminé (ajusté ou non), l'entité est classée selon le barème suivant :
•**Score < 1,75** : Risque faible (1)
•**1,75 ≤ Score < 2,5** : Risque moyen (2)
•**2,5 ≤ Score < 3,25** : Risque substantiel (3)
•**Score ≥ 3,25** : Risque élevé (4)

Évaluation et classification de la qualité des contrôles LCB/FT mis en place par les entités assujetties (Indicateurs en Annexe I Section B) :

Sur la base de ce score, l'entité est classée comme suit :
Score < 1,75 : Très bonne qualité des contrôles (A)
1,75 ≤ Score < 2,5 : Bonne qualité des contrôles (B)
2,5 ≤ Score < 3,25 : Qualité moyenne des contrôles (C)
Score ≥ 3,25 : Mauvaise qualité des contrôles (D)

Évaluation et classification du profil de risque résiduel des entités assujetties (combinaison des 2 premiers indicateurs)

Sur la base du score de risque résiduel obtenu, les autorités classent l'entité selon les seuils suivants :
Score < 1,75 : Risque faible (1)
1,75 ≤ Score < 2,5 : Risque moyen (2)
2,5 ≤ Score < 3,25 : Risque substantiel (3)
Score ≥ 3,25 : Risque élevé (4)

Évaluation du risque au niveau du groupe :

- En agrégeant les scores de risque résiduel au niveau de chaque entité composant le groupe via des moyennes pondérées
- L'importance de chaque entité est évaluée à partir des points de données figurant à l'annexe I, section A en se fondant sur :

(i) le nombre total de clients ;
(ii) la valeur totale en euros des transactions entrantes et sortantes ;
(iii) le montant total des actifs détenus ou gérés.

Le résultat de l'agrégation est converti en **score numérique de risque résiduel du groupe** :
Score < 1,75 : Risque faible (1)
1,75 ≤ Score < 2,5 : Risque moyen (2)
2,5 ≤ Score < 3,25 : Risque substantiel (3)
Score ≥ 3,25 : Risque élevé (4)

$$\left(\sum_{i=1}^{N} w[i]r[i]^{\alpha}\right)^{\frac{1}{\alpha}}$$

Where:

N: number of entities in the group

r[i]: residual risk score of entity i

w[i]: weight representing the relevance of entity i within the group

$\alpha \geq 1$: parameter to enhance the contribution of risker entities

Méthode de calcul de l'évaluation du risque groupe

Détails du RTS N°3

regulation partners

RTS sur la vigilance à l'égard de la clientèle (CDD)

Références : Article 28(1) du Règlement (UE) 2024/1624 – AMLR

Objectif :
Ce RTS se concentre sur l'étendue et la qualité des informations que les institutions devront obtenir dans le cadre de leur processus de vigilance à l'égard de la clientèle dans le cadre du nouveau régime de LCB-FT. Afin d'obtenir des résultats efficaces et de limiter les coûts de conformité, l'ABE propose un cadre permettant aux institutions de choisir l'approche la plus appropriée, dans la mesure où elle est conforme au nouveau règlement LCB-FT.

Contenu du RTS :

• Section 1 : CDD standard : les informations que les entités assujetties seront tenues de collecter en vue d'identifier et de vérifier l'identité des clients et bénéficiaires effectifs, et de comprendre la structure de propriété et de contrôle du client, ainsi que les sources d'information qui peuvent être utilisées à ces fins

•Section 2 : mesures à mette en œuvre pour identifier et comprendre l'objet et la nature de la relation d'affaires

•Section 3 : mesures spécifiques liées à l'identification des personnes politiquement exposées

•Section 4 : mesures sectorielles qui peuvent être mises en œuvre s'agissant des mesures vigilance simplifiées (Exigences allégées dans certains cas (ex : fonds collectifs, comptes de cantonnement)

•Section 5 : exigences additionnelles applicables en cas de vigilance renforcée (Informations supplémentaires sur l'origine des fonds, des bénéficiaires, des associés)

•Section 6 : Sanctions financières ciblées

•Section 7 : Facteurs de risque associés aux caractéristiques des instruments de monnaie électronique

•Section 8 : Moyens d'identification électronique et services de confiance qualifiés pertinents

Après (AMLR + RTS Article 28)

- Standardisation précise des informations à collecter
- Cadre encadré et sécurisé pour la vérification à distance
- Délai clair (les entités doivent toujours détenir des données d'identification à jour et actualiser les informations pour les clients existants dans un délai de 5 ans suivant l'application du Règlement)
- Souplesse explicite et obligation d'inclusion numérique
- Réduction des distorsions réglementaires et concurrentielles intra-UE

Détails du RTS N°3

Contenu du RTS

Section 1 – Identification et vérification (Art. 1-14)
•**Art. 1 à 3** : Informations sur le nom, l'adresse, lieu de naissance (PP), dénomination sociale ou/et nom commercial (PM)
•**Art. 4 à 5** : Nationalités + documents d'identité exigés.
•**Art. 6** : Identification à distance (solutions eIDAS niveau « substantiel » ou « élevé »).
•**Art. 7** : Sources fiables et indépendantes (l'entité doit examiner la fiabilité de ses sources)
•**Art. 8** : IBAN virtuel – transmission des infos entre établissements afin d'identifier la PP ou PM utilisatrice
•**Art. 9 à 10** : Vérification des bénéficiaires effectifs et compréhension de la structure de propriété et contrôle client (ex : lorsque la structure de propriété comprend plusieurs entités ou arrangements)
•**Art. 11 à 14** : Structures complexes (organigrammes exigés), dirigeants, fiducies et fiducies discrétionnaires.

Section 2 – Nature et objet de la relation d'affaires (Art. 15-16)
•Collecte d'informations sur l'objet, le volume des flux, la source/destination des fonds et la nature de la relation d'affaires ou des opérations occasionnelles

Section 3 – Personnes politiquement exposées (Art. 17)
•(À réaliser avant l'EER art 17-1-a) Obligation de vérification automatisée ou combinée (screening PEP, famille, associés) sauf si la taille, le modèle d'affaires, la complexité ou la nature de l'entité permet des vérifications manuelles uniquement (art 17-2)

Section 4 – Diligence simplifiée (Art. 18-23)
•Détails des exigences minimales en cas de risque faible, notamment pour :

- Identification simplifiée
- Vérification des bénéficiaires effectifs
- Comptes collectifs, OPCVM
- Nature de la relation
- La fréquence de Maj des données d'identification dans les situations à faible risque

Détails du RTS N°3

Section 5 – Diligence renforcée (Art. 24-27)

•Collecte d'informations supplémentaires sur :

- Le client et les bénéficiaires
- La nature de la relation d'affaires
- La source des fonds et du patrimoine
- Le but des opérations envisagées ou effectuées

Section 6 – Sanctions financières ciblées (Art. 28-29)

- Screening obligatoire via des outils automatisés (sauf si la taille, le modèle d'affaires, la complexité ou la nature de l'entité permet des vérifications manuelle) sur :
- tous les prénoms et noms de famille + date de naissance (PP)
- nom de la personne morale (PM)
- dans le cas d'une PP, PM, organisme ou entité : tous autres noms, pseudonymes, noms commerciaux, adresses de portefeuilles, lorsqu'ils figurent dans les listes de sanctions financières ciblées
- dans le cas d'une PM : les informations sur les bénéficiaires effectifs.
- en cas de match, comparer les informations visées à ce point avec toutes les informations disponibles issues des diligences raisonnables concernant le client ou le bénéficiaire effectif, afin de déterminer si la personne est bien la cible visée par les sanctions financières ciblées. En cas de doute, l'entité assujettie doit se référer à toutes les autres sources d'information disponibles (sources publiques, ex : registres des entités détenues et contrôlées et les registres centraux)
- vérification régulière des clients et des bénéficiaires effectifs, au moins :
- lors de l'EER avec le client ou avant d'établir une relation d'affaires ou d'effectuer une opération occasionnelle
- lorsqu'un changement survient dans l'une des désignations existantes, ou lorsqu'une nouvelle désignation est effectuée conformément à l'article 26(4) du Règlement (UE) 2024/1624 ;
- si des modifications significatives interviennent dans les données de vigilance client existantes, concernant le client ou le bénéficiaire effectif (changement de nom, résidence, nationalité ou une modification des activités commerciales)
- veiller à ce que la vérification ainsi que la validation soient effectuées à l'aide de listes de sanctions financières ciblées à jour, sans retard indu

Section 7 – Facteurs de risques liés aux instruments de Monnaie électronique (Art. 30)

•Facteurs de réduction du risque : plafonds, canaux limités, instruments prépayés.

Section 8 – Identification électronique (Art. 31-32)

•Liste des attributs requis pour les services de confiance qualifiés (Annexe I).

•Obligation de compléter les attributs manquants via d'autres moyens.

(Article 32) Entrée en vigueur :

- Entre en vigueur le 20e jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.
- L'article 23, paragraphe 1, s'applique aux clients déjà existants ainsi qu'aux nouveaux clients à intégrer après l'entrée en vigueur du présent règlement. Pour les clients déjà existants, les informations visées à l'article 23, paragraphe 1, doivent être mises à jour selon une approche fondée sur les risques, et au plus tard cinq ans après l'entrée en vigueur du présent règlement (obligatoire dans tous ses éléments et directement applicable dans tous les États membres)

Détails du RTS N°4

RTS sur les sanctions pécuniaires, mesures administratives et astreintes

Référence : Article 53(10) de la Directive (UE) 2024/1640 – AMLD6

Ce RTS se concentre sur les indicateurs et critères à prendre en compte lors de la fixation du niveau des sanctions pécuniaires ou de la prise de mesures administratives, y compris l'élaboration d'une méthodologie d'imposition d'astreintes. L'objectif est de garantir que les violations de la LBC/FT soient évaluées de manière uniforme par tous les superviseurs de l'UE et que les mesures coercitives soient proportionnées, dissuasives et efficaces.

AMLD6 + RTS Article 53

- Niveau d'harmonisation inédit à l'échelle européenne
- Méthodologie fondée sur des indicateurs partagés
- Introduction des PePPs, outil à visée corrective
- Critères explicites pour moduler les montants de sanctions
- Ambition claire : des sanctions plus dissuasives et crédibles

Contenu du RTS :

- **Section 1 (art 1 – 3) : Classification des infractions** :
  - 4 niveaux de gravité (mineur à très grave).
  - Liste d'indicateurs
  - Voir en détail la slide 12

- **Section 2 : Critères pour fixer les sanctions :**
  - Alignés avec ceux de l'AMLA
  - A prendre en compte en plus des indicateurs (art 1 – 3)
  - Réduction du montant :
    - Coopération avec l'entité
    - Comportement correctif après découverte
    - Autres critères identifiés par l'autorité
  - Augmentation du montant :
    - Absence de coopération
    - Absence de mesures correctives
    - Responsabilité élevée (ex : grave négligence)
    - Bénéficie tiré du manquement
    - Préjudices causés à des tiers
    - Antécédents de non-conformité ou sanctions
    - Autres critères identifiés par l'autorité
  - Pour les PP non directement assujettie, rendre en compte :
    - Leur rôle
    - L'étendu de leur responsabilité
  - Pour les PM et PP, prendre en compte lors des sanctions :
    - PM : CA, états financiers, fonds propres et liquidité
    - PP : revenu annuel, rémunération (fixe et variable)

- **Section 3 : Méthodologie des astreintes (PePPs) :**
  - Outil nouveau au niveau européen
  - Vise à forcer une entité à corriger une non-conformité
  - Encadrée : procédure contradictoire, durée max, délai d'exécution

- **(Article 11) Entrée en vigueur :** Le présent règlement entre en vigueur le vingtième jour suivant sa publication au Journal officiel de l'Union européenne.
  Il s'applique à partir du 10 juillet 2027

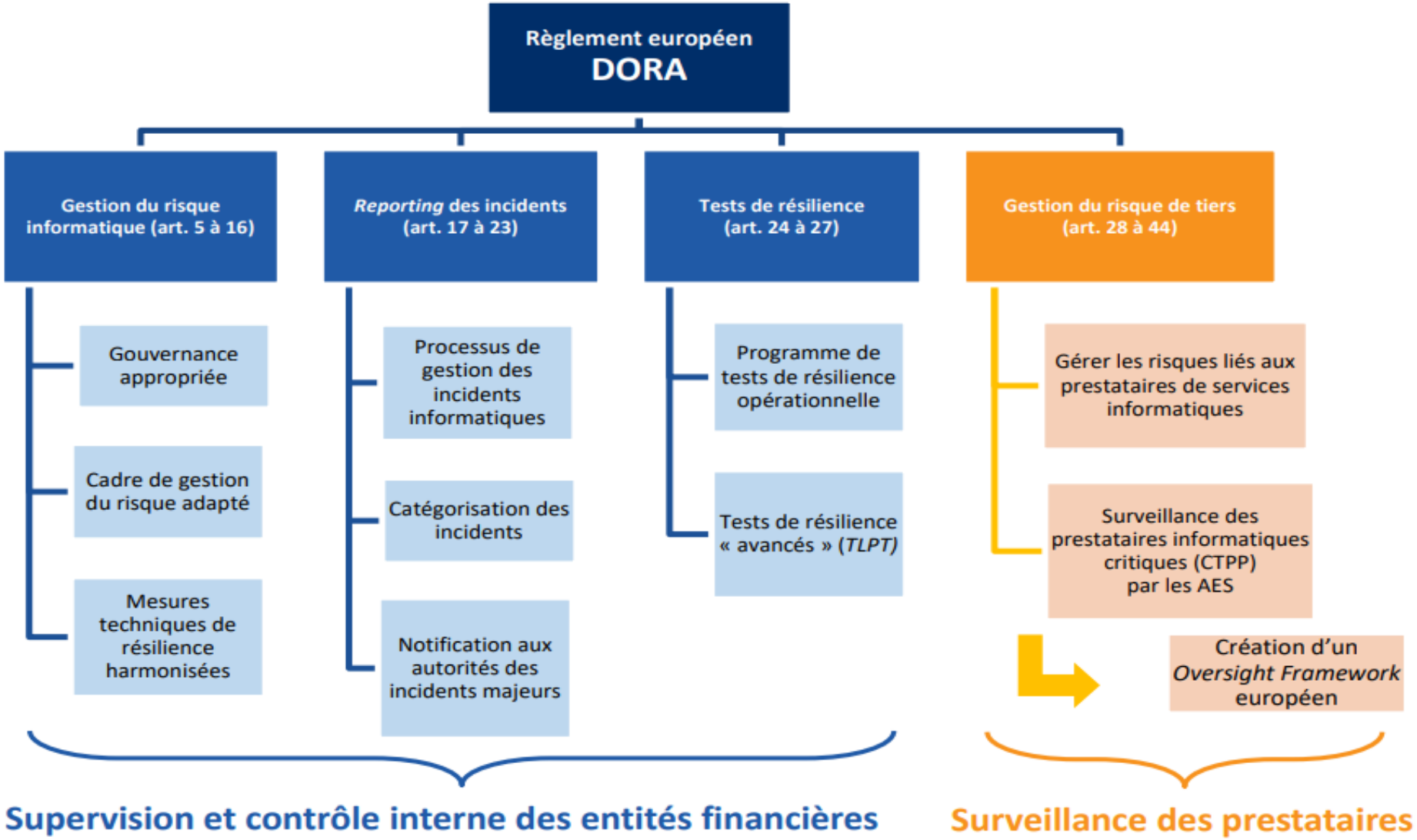
Détails du RTS N°4

tableau récapitulatif des indicateurs de gravité des manquements et leur classification selon le niveau de gravité (1 à 4) tel que défini par les Articles 1 et 2 du présent RTS :			
Lettre	**Indicateurs**	**Catégorie concernée**	**Critère d'interprétation**
a)	Durée du manquement	1 à 3	Courte = catégorie 1 ; Longue = catégorie ≥3
b)	Répétition du manquement	1 à 3	Non répété = catégorie 1 ; Répété = catégorie ≥3
c)	Comportement de la personne responsable	Tous niveaux	Considéré dans l'analyse qualitative globale
d)	Impact sur l'entité assujettie (local, groupe, transfrontalier ; clients ; systèmes LBC/FT)	Cat. 1 à 4	Mineur = cat. 1 ; Modéré = cat. 2 ; Significatif = cat. 3 ; Très significatif = cat. 4
e)	Impact sur l'exposition aux risques BC/FT	Cat. 1 à 4	Même logique que d)
f)	Nature du manquement (type d'obligation violée)	Tous niveaux	Indicateur à considérer qualitativement dans la classification
g)	Facilitation d'activités criminelles	Catégorie 4	Si rempli → classement en catégorie 4
h)	Défaillance structurelle ou absence de dispositifs LBC/FT	Catégorie 4	Si rempli → classement automatique en catégorie 4
i)	Impact sur la viabilité financière de l'entité ou du groupe	Catégorie 4	Si impact réel ou potentiel significatif
j)	Impact sur le système financier ou les marchés	Catégorie 4	Si impact sur intégrité, stabilité ou bon fonctionnement
k)	Caractère systématique du manquement	Catégorie ≥3	Si systématique → au moins catégorie 3
l)	Autres indicateurs identifiés par l'autorité	Variable	À l'appréciation de l'autorité compétente

tableau récapitulatif des indicateurs de gravité des manquements et leur classification selon le niveau de gravité (catégories 1 à 4) tel que défini par les Articles 1 et 2	
catégorie	**Critères caractéristiques**
1	Si impact mineur ou inexistant (indicateurs d et e), qu'il est de courte durée, non répété, et qu'aucun des indicateurs g à k n'est rempli.
2	Si 'impact est modéré (d et e) et qu'aucun des indicateurs g à k n'est rempli.
3	Si impact est significatif (d et e) et que le manquement est de longue durée, répété ou systématique.
4	Si impact est très significatif (d et e), si l'indicateur h est rempli, ou encore si : – l'indicateur g montre une facilitation ou implication dans des activités criminelles significatives *et/ou* – les indicateurs i ou j révèlent un impact significatif.

Le Règlement sur la résilience opérationnelle numérique (DORA)

Préambule


Règlement européen
DORA
Gestion du risque informatique (art. 5 à 16)
Reporting des incidents (art. 17 à 23)
Tests de résilience (art. 24 à 27)
Gestion du risque de tiers (art. 28 à 44)
Gouvernance appropriée
Cadre de gestion du risque adapté
Mesures techniques de résilience harmonisées
Processus de gestion des incidents informatiques
Catégorisation des incidents
Notification aux autorités des incidents majeurs
Programme de tests de résilience opérationnelle
Tests de résilience « avancés » (*TLPT*)
Gérer les risques liés aux prestataires de services informatiques
Surveillance des prestataires informatiques critiques (CTPP) par les AES
Création d'un *Oversight Framework* européen
Supervision et contrôle interne des entités financières
Surveillance des prestataires

Préambule

TEXTES DE NIVEAU 2 : RTS (Regulation Technical Standards)

- CADRE DE GESTION DES RISQUES LIES AUX TIC & D'UN CADRE DE GESTION SIMPLIFIE
- CRITERES DE CLASSIFICATION DES INCIDENTS LIES AUX TIC
- REGISTRE D'INFORMATION & POLITIQUE LIEE AUX SERVICES TIC EFFECTUES PAR DES TIERS
- DECLARATION DETAILLEE DES INCIDENTS MAJEURS LIES AUX TIC
- TESTS D'INTRUSION BASES SUR LES MENACES (TLPT)
- ELEMENTS A EVALUER OU A DETERMINER LORS DE LA SOUS TRAITANCE DE SERVICES LIES AUX TIC SOUTENANT UNE FONCTION CRITIQUE OU IMPORTANTE
- HARMONISATION DES CONDITIONS DE SURVEILLANCE

TEXTES DE NIVEAU 2 : ITS (Implementation Technical Standards)

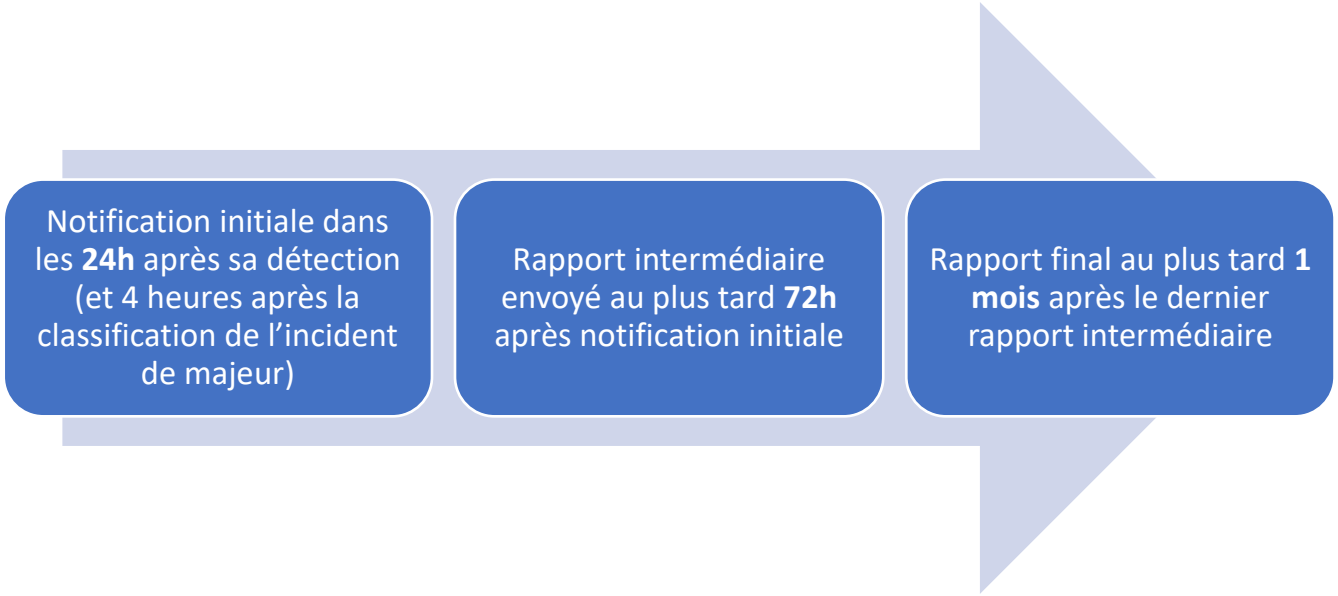
- ITS SUR LES MODELES DU REGISTRE D'INFORMATION
- ITS SUR LE CONTENU, LES DELAIS & MODELES DE RAPPORTS DES INCIDENTS & CYBER ATTAQUES

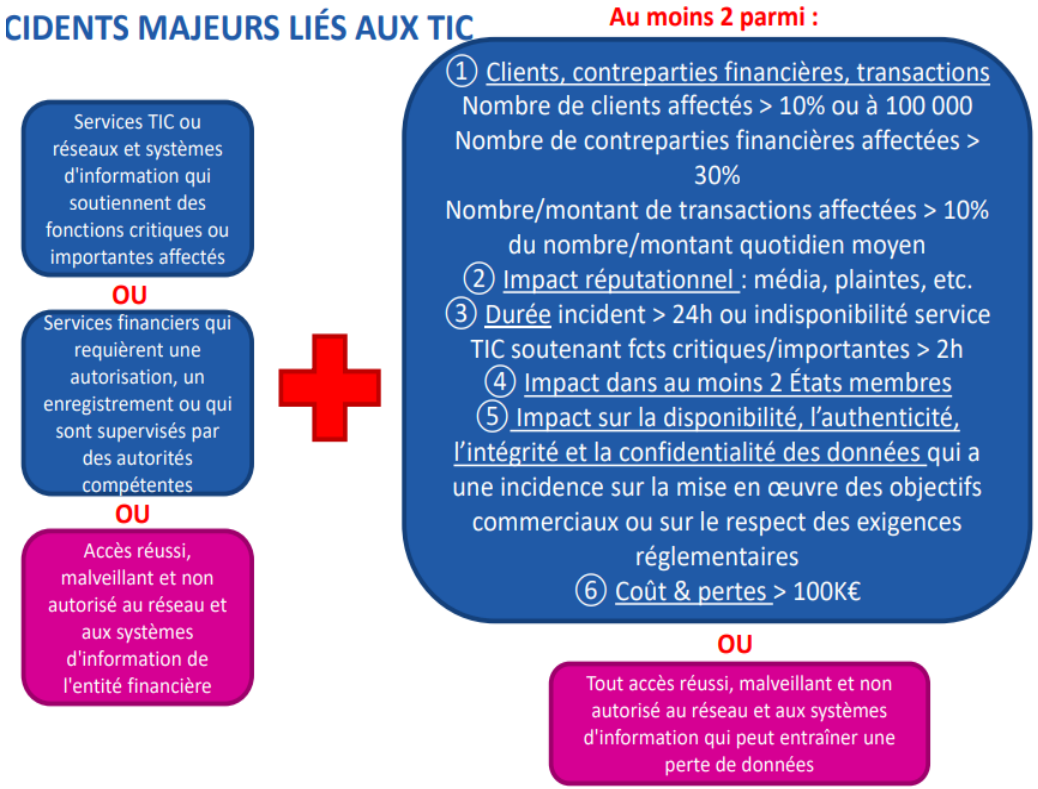
TEXTES DE NIVEAU 3 : GUIDELINES (Orientations)

- ORIENTATION SUR LA GESTION DES RISQUES LIES AUX TIC ET A LA SECURITE
- ORIENTATIONS SUR LES COUTS ET LES PERTES LIES AUX INCIDENTS MAJEURS

Gestion, classification et notification des incidents liés à la gestion informatique

L'entité financière doit notifier l'incident majeur à l'ACPR dans un délai de 4 heures après l'avoir classé comme un incident majeur et dans tous les cas au plus tard dans les 24 heures suivants la découverte de l'incident.





TLPT(Threat-Led Penetration Testing) : Qui est concerné ?

L'identification des entités à tester, par la/les autorité(s) TLPT compétente(s), se fait dans le cadre d'un plan triennal (sauf exceptions, la fréquence et le planning des tests étant fixés par la/les autorité(s) TLPT compétente(s)). Le fait qu'une entité en principe éligible au regard des critères quantitatifs du RTS DORA TLPT ne soit pas désignée sur le 1er cycle triennal ne signifie pas qu'elle ne le sera pas sur les cycles suivants.

ETABLISSEMENT DE CRÉDIT

Identifiés comme Établissement d'importance systémique mondiale

ETABLISSEMENT DE PAIEMENT

Ainsi que les Établissements de Monnaie Électronique (EME), dépassant 120 milliards d'euros au cours de chacun des deux exercices précédents la valeur totale des opérations de paiement

DÉPOSITAIRES CENTRAUX DE TITRES (DCT)

Il s'agit des infrastructures essentielles au bon fonctionnement et à la sécurité des marchés d'instruments financiers

LES CONTREPARTIES CENTRALES (CCP)

Entités financières qui interviennent dans les transactions sur les marchés financiers

PLATEFORMES DE TRADING

Sont concernées les plateformes les plus sensibles au niveau national ou européen

LES ENTREPRISES D'ASSURANCE ET DE RÉASSURANCE

L'examen du règlement délégué sur les TLPT, adopté le 13 février par la Commission européenne et soumis à un droit de regard du Parlement européen d'une durée de 3 mois est termine. Il a été publié le 18 juin

Focus sur le Règlement délégué (UE) 2025/1190 de la Commission du 13 février 2025

regulation partners

Cadre général et organisation des TIFM

Contexte réglementaire :

- Complète le **règlement (UE) 2022/2554 (DORA)**.
- Publié au JOUE le **18 juin 2025**, repose sur le cadre **TIBER-EU**.
- Définit les **critères**, **exigences**, **phases**, et **coopérations** des **tests d'intrusion fondés sur la menace (TIFM)**.

Entités concernées :

- entités citées à l'article 2 du Règlement DORA, seulement si sélectionnée :
- sur l'**impact**, le **caractère systémique** et le **risque TIC**.
- Notification officielle → lancement obligatoire du TIFM.

Organisation du test:

- Désignation par l'autorité TIFM :
  - d'un **gestionnaire de test** (+ suppléant),
  - d'une **équipe de cybersécurité TIFM**.
- L'entité financière désigne une **équipe de contrôle**, avec un chef responsable.
- Préparation (sous 3 à 6 mois)*

*L'entité financière dispose de 3 mois pour communiquer aux gestionnaires de test toutes les informations suivantes concernant le lancement du TIFM :

- une charte de projet comprenant un plan de projet de haut niveau, contenant les informations visées à l'annexe I du règlement ;
- les coordonnées du chef de l'équipe chargée du contrôle ;
- des informations sur le recours prévu à des testeurs internes ou externes, ou les deux, le cas échéant ;
- des informations sur les canaux de communication à utiliser pendant le TIFM ;
- le nom de code du TIFM.
- Document de spécification du périmètre du test (dans un délai de 6 mois à compter de la réception de la notification initiale)

Focus sur le Règlement délégué (UE) 2025/1190 de la Commission du 13 février 2025

regulation partners

Déroulement, validation et suivi du TIFM

Phases de test :

- **Équipe rouge** : simule les attaques (durée min. 12 semaines).
- **Équipe bleue** : défend et réagit, composée du personnel de l'entité.
- Utilisation de **3 scénarios de menace** issus d'un rapport de renseignement (Annexe III).

Livrables et délais :

- Rapport équipe rouge : sous 4 semaines.
- Rapport équipe bleue : sous 10 semaines.
- Exercice de collaboration violette : analyse croisée.
- Rapport de synthèse final : 8 semaines après validation.
- Plans correctifs + attestation finale délivrée par l'autorité TIFM.

Aspects spécifiques :

- Tests groupés ou communs : coordination entre plusieurs entités.
- Coopération multi-États : reconnaissance mutuelle organisée.
- Sélection stricte des testeurs – modalités précisées dans le règlement.

Sous 10 semaines après la fin de la phase active de test de l'équipe rouge, l'équipe bleue et les testeurs rejouent les actions offensives et défensives menées pendant le TIFM. L'équipe chargée du contrôle mène également un exercice de « collaboration violette » sur des sujets déterminés conjointement par l'équipe bleue et les testeurs, sur la base des vulnérabilités recensées lors du test et, le cas échéant, sur des questions qui n'ont pas pu être testées au cours de la phase active de test de l'équipe rouge.

Le Règlement européen sur l'intelligence artificielle (IA Act)

L'IA ACT

regulation partners

L'IA Act

- Les 27 États membres de l'Union européenne réunis à Bruxelles ont validé l'AI Act le **2 février 2024**
- Entrée en vigueur du règlement le **1er août 2024**

Approche par les risques

- Classification en 3 niveaux de risque : **risque « inacceptables », risque « élevé », risque « modéré ».**

Contrôle des pratiques IA dans l'UE

- Système de gouvernance au niveau des États membre.
- Création d'un *Bureau de l'IA*.

Sanctions fortes

- 35 millions d'euros ou à 7 % du CA pour les violations des applications d'IA interdites.
- 15 millions d'euros ou à 3 % du CA pour les violations des obligations découlant de la législation sur l'IA.
- 7,5 millions d'euros ou à 1 % du CApour la communication d'informations inexactes, incomplètes ou trompeuses.

Calendrier mise en oeuvre

- **Depuis le 2 février 2025** :
  - Obligation générale de formation applicable aux fournisseurs de systèmes d'IA, déployeurs (entreprises qui utilisent un système d'IA, même développé par un tiers) et utilisateurs (salariés, sous-traitants ou partenaires exploitant ces systèmes).
  - Les SIA présentant des risques jugés inacceptables sont interdits.
- **Depuis le 2 mai 2025** :
  - Publication des Codes de bonnes pratiques en matière d'IA à usage general par les fournisseurs qui permettent de montrer leur conformité à l'article 53 (cf slide suivant)
- **A partir du 2 aout 2025** :
  - Désignation des autorités notifiantes
  - Entrée en vigueur des règles pour les modèles d'IA à usage general

«**modèle d'IA à usage général**», un modèle d'IA, y compris lorsque ce modèle d'IA est entraîné à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle, qui présente une généralité significative et est capable d'exécuter de manière compétente un large éventail de tâches distinctes, indépendamment de la manière dont le modèle est mis sur le marché, et qui peut être intégré dans une variété de systèmes ou d'applications en aval, à l'exception des modèles d'IA utilisés pour des activités de recherche, de développement ou de prototypage avant leur mise sur le marché;

- **A partir du 2 août 2026: obligations liées aux systèmes d'IA à haut risque**

Obligations IA à usage general (applicables août 2025)

Les fournisseurs de modèles d'IA à usage général:

a) élaborent et tiennent à jour la documentation technique du modèle, y compris son processus d'entraînement et d'essai et les résultats de son évaluation, qui contient, au minimum, les informations énoncées à l'annexe XI aux fins de la fournir, sur demande, au Bureau de l'IA et aux autorités nationales compétentes;

b) élaborent, tiennent à jour et mettent à disposition des informations et de la documentation à l'intention des fournisseurs de systèmes d'IA qui envisagent d'intégrer le modèle d'IA à usage général dans leurs systèmes d'IA.

c) mettent en place une politique visant à se conformer au droit de l'Union en matière de droit d'auteur et droits voisins,

d) élaborent et mettent à la disposition du public un résumé suffisamment détaillé du contenu utilisé pour entraîner le modèle d'IA à usage général, conformément à un modèle fourni par le Bureau de l'IA

Obligations clés pour les systèmes d'IA à haut risque (IA Act, chap. III, sec. 2)-

- **Gestion des risques (art. 9)** : Identification, évaluation et réduction continue des risques tout au long du cycle de vie.
- **Qualité et gouvernance des données (art. 10)** : Données fiables, représentatives, exemptes de biais, avec traçabilité.
- **Documentation technique (art. 11)** : Dossier complet décrivant les objectifs, performances et limites du système.
- **Enregistrement (art. 12 & 49)** : Inscription obligatoire dans la base de données de l'UE avant mise sur le marché.
- **Transparence (art. 13)** : Informations claires et accessibles pour les utilisateurs/déployeurs.
- **Contrôle humain (art. 14)** : Supervision effective, possibilité d'intervenir ou désactiver le système.

Actualités

- **Lignes directrices sur les SIA interdits** : Publication le 2 février 2025, la CE a publié des lignes directrices clarifiant les pratiques d'IA interdites (Article 5)

- **Lignes directrices sur la définition des SIA** : Publication le 2 février 2025, la CE a publié des lignes directrices visant à aider à définir si un logiciel constitue un SIA. Cette définition s'apprécie au regard de l'autonomie du système, sa capacité à générer des inférence à partir de données et à évoluer après son déploiement.

- **Retrait de la directive sur la responsabilité de l'IA** : Le 11 février 2025, la CE décide de retirer la Directive sur la responsabilité en matière d'intelligence artificielle par l'absence de besoin d'un cadre juridique actuel avec la mise à jour de la Directive sur les produits défectueux (Directive (UE) 2024/2853)

Contact

Marie-Agnès Nicolet - Présidente fondatrice
Regulation Partners
30, rue La Boétie - 75008 Paris
marieagnes.nicolet@regulationpartners.com