Digital Operational Resilience Act (DORA)

Réglement UE 2022/2554 du 14 décembre 2022

Maya Coumes & Camille Saettel
Regulatory – Digital Business

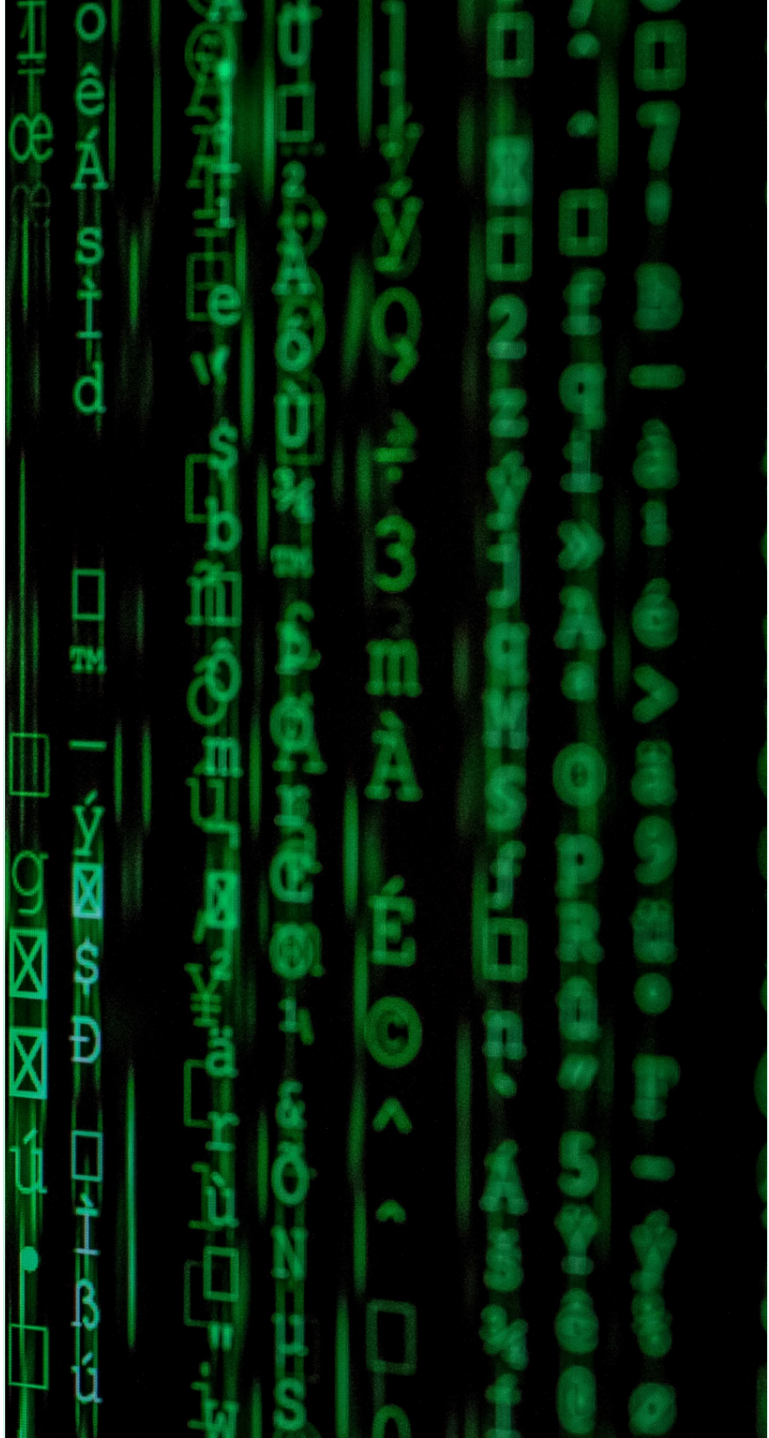
22 Mai 2024

Introduction

- Pourquoi ?
  - Numérisation de l'activité financière / assurances
  - Augmentation de l'externalisation
  - Risque systémique du à l'interconnexion
  - Fragmentation de la réglementation

- Résilience = continuité des activités

- Prévention des risques internes, externes et systémiques



Introduction

Structure

- DORA comporte 5 piliers

  - ❑ Gestion du risqué lié aux TIC (Chapitre II)
  - ❑ Gestion, classification et notification des incidents liés aux TIC (Chapitre III)
  - ❑ Test de résilience opérationnelle numérique (Chapitre IV)
  - ❑ Gestion des risques liés aux prestataires de services TIC (Chapitre V)
  - ❑ Dispositif de partage d'information (Chapitre VI)

Introduction

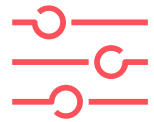
Champ d'application

Entités financières: 20 types d'entités

- Etablissements de crédit
- Etablissements de monnaie électronique
- Gestionnaire de fonds d'investissements
- Sociétés de gestion
- Entreprises d'assurances / réassurance
- …

➢ PSF : NON

PSF de support (ICT)
PSF spécialisés



Prestataires tiers de services TIC
entreprise fournissant des services de TIC

Ex : cloud, logiciels, services d'analyses de données, infrastructures de paiement

Y inclus intragroupe, et entités financières qui fournissent des services à d'autres entités financières;

Introduction
Concepts clés

- Principe de proportionnalité
  - Définition du risque **et** supervision ;
  - Cadre simplifié de gestion du risque ; microentreprises

- Principe de responsabilité (*accountability*) / liability

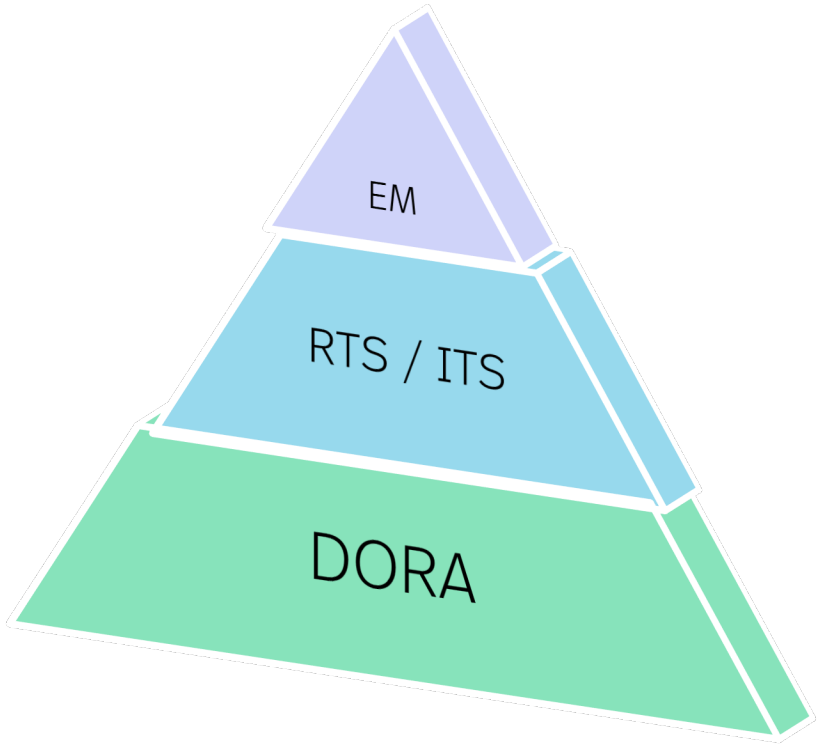
- Fonctions critiques et importantes (CIF):

fonction dont la perturbation est susceptible de nuire sérieusement à la performance financière d'une entité financière, à la continuité de ses activités, ou à sa capacité à respecter les conditions de son agrément

Quid notions voisines ?
CSSF 22/806

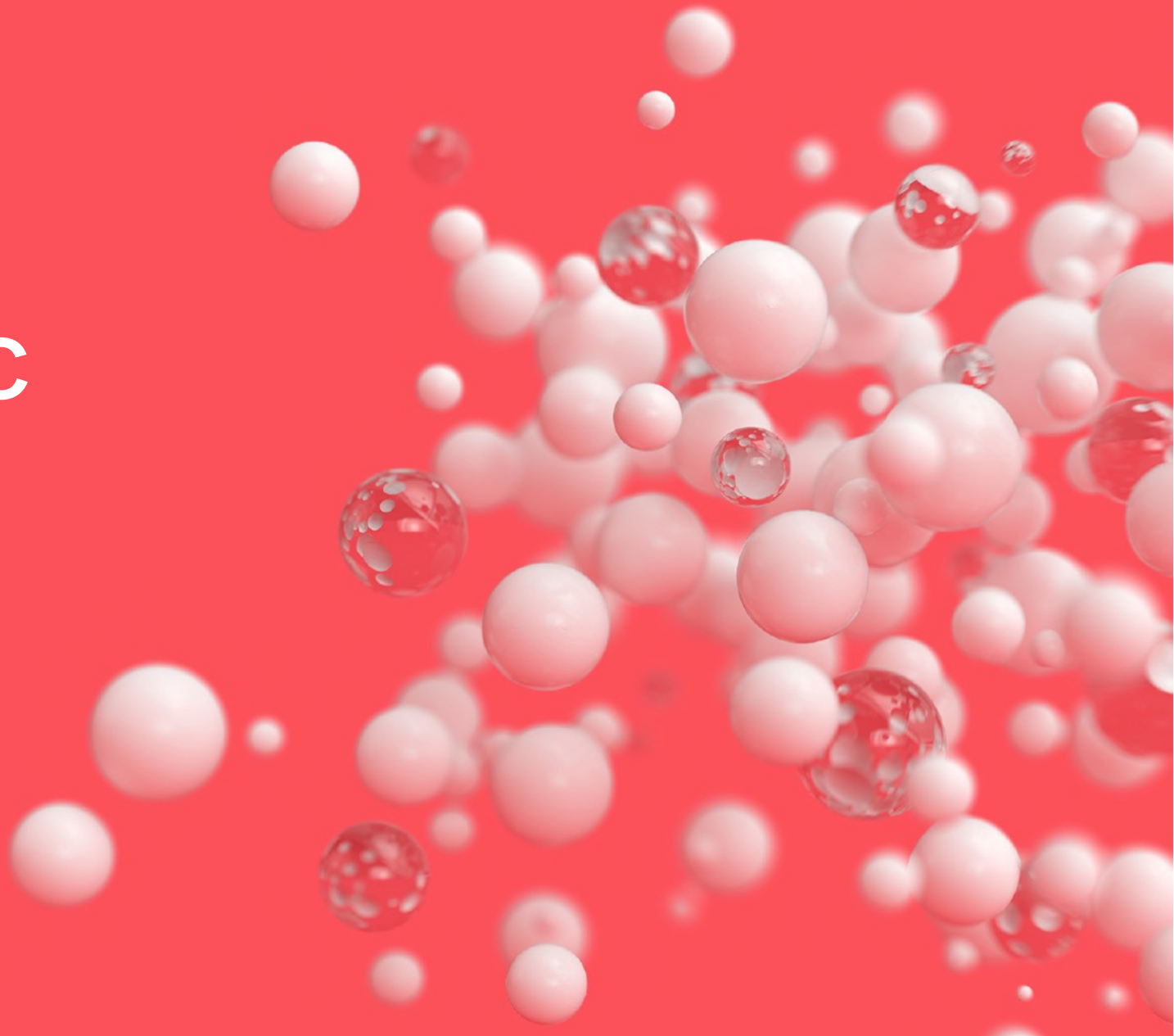
Introduction
Composition

- DORA est composé de plusieurs niveaux de textes
  - Niveau 1 : DORA
  - Niveau 2 : RTS / ITS
    - 1st batch RTS (adoptés)
    - 2nd batch RTS (en cours)
  - Mesures nationales: Projet de loi 8291 (4.08.23)



Pilier I

Gestion du risque TIC



Pilier I – le cadre de gestion du risque TIC

Art. 6
Stratégies, politiques, procédures, protocoles, outils de TIC incluant les stratégies de résilience opérationnelle numérique

Identification :

- Fonction “métier”, rôles et responsabilités
- Fonction critique et importante (CIF)
- Sources de risques
- Des prestataires de services tiers TIC

Détection : mise en place de mécanismes de détection

Réponse et rétablissement : politique complète de continuité des activités de TIC

PRINCIPE DE PROPORTIONALITE

Art. 16 DORA
–
cadre simplifié de gestion

Pilier I – le cadre de gestion du risque TIC

Gouvernance et Responsabilité

(Art. 5)

- Responsabilité de l'organe de direction qui approuve, supervise le cadre de gestion du risque et définit le niveau de tolérance au risque
- Membre de la direction désigné pour superviser l'exposition au risque
- 3 lignes de défense
- Fonction de contrôle (indépendante)
- Mise en place de canaux de notification
- Formations régulières

PRINCIPE DE PROPORTIONNALITE

Pilier I – le cadre de gestion du risque TIC

Résumé et questions pratiques

Les prochaines étapes à accomplir

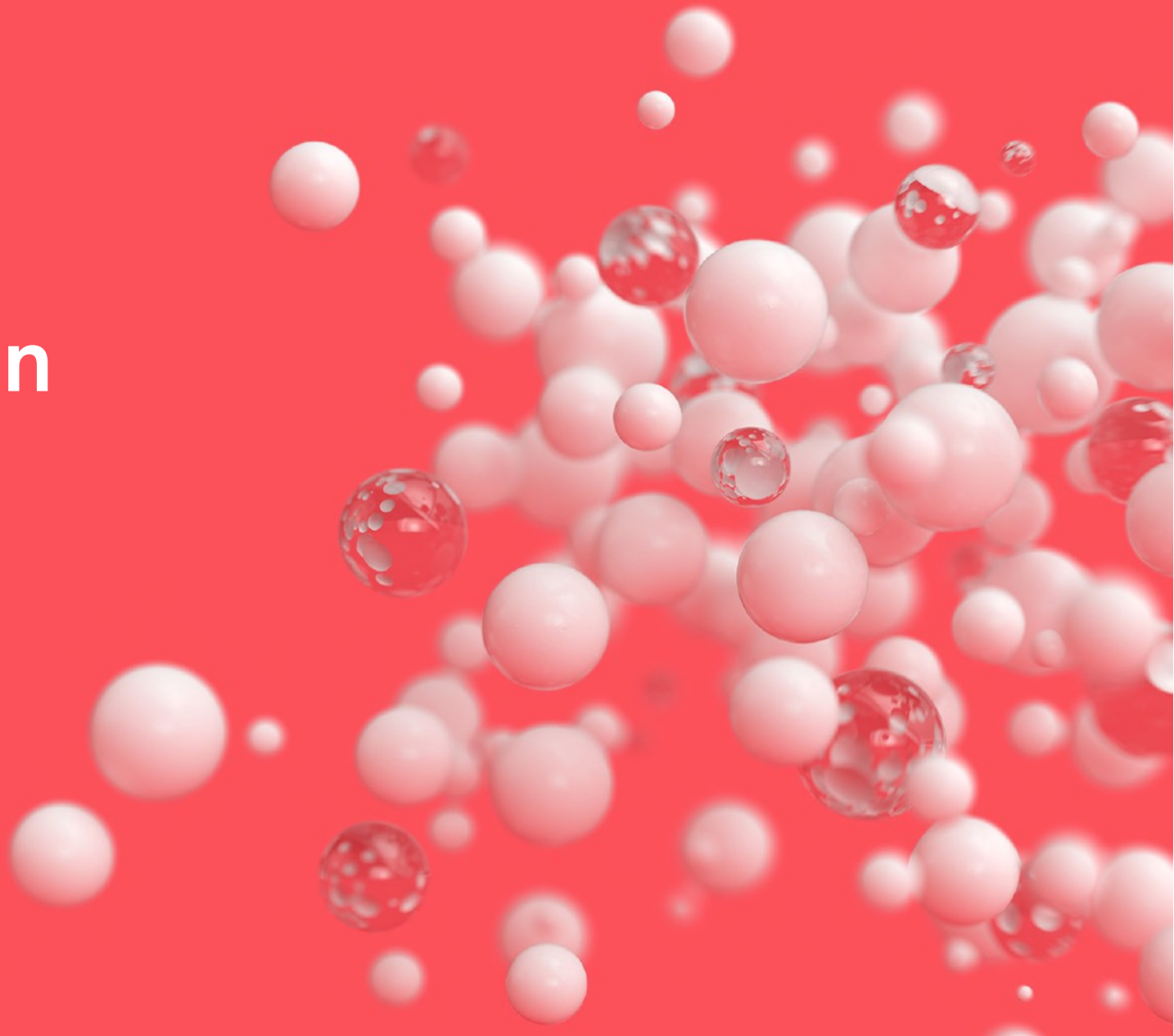
- Identification (maping)
- Mise à jour ou création des procedures appropriées
- Concertation de l'organe de direction sur les aspects gouvernance
- Création d'une fonction dédiée ou necessité de s'interroger sur la dépendance de la fonction en place
- Revue du cadre de formation instauré au sein de l'entité pour y intégrer DORA

Quelques questions pratiques

- Intra-groupe: Le groupe conduit la compliance avec DORA, puis-je me reposer sur le travail fait au niveau du groupe?
- La fonction contrôle peut-elle être exercée au niveau du groupe? Faut-il notifier cette fonction à la CSSF?

Pilier II

Gestion, classification et notification des incidents TIC



Pilier II – Gestion, classification et notification des incidents TIC

- Circulaire CSSF 24/847
- NIS 1 (OSE)
- NIS 2
- DORA : *Lex specialis*

Circulaire CSSF 11/504

Abrogée

Circulaire CSSF 24/847

Entrée en vigueur

01 avril 2024 = E.C OSE
01 juin 2024 = OPC & SDG

DORA

Application

17 Janvier 2025

Pilier II – Gestion, classification et notification des incidents TIC

<u>1ère étape : Classification des incidents selon les critères suivants</u> RTS

- Nombre de clients (>10% des clients qui utilisent le service impacté ou >100 000 clients impactés)
- Durée de l'incident (+24h ou arrêt +2h)
- Répartition géographique
- Pertes de données occasionnées
- Criticité des services touchés
- Conséquences économiques (>100K EUR)

<u>2è étape : Identification des incidents majeurs</u> RTS

- Fonctions critiques et importantes affectées par l'incident

et

Alternativement :

- ➢ Soit un accès non autorisé aux systèmes d'information
- ➢ Soit les seuils de signification de deux autres critères sont atteints

Pilier II – Gestion, classification et notification des incidents TIC

Le régime de notification

- **Notification obligatoire** des incidents majeurs aux régulateurs RTS
  - Notification initiale (+4h ; max 24h)
  - Rapport intermédiaire (72h)
  - Rapport final (1 month)
- Notification **obligatoire** des clients (incidence sur les intérêts financiers)
- Notification **volontaire** des cybermenaces importantes aux régulateurs
- Notification des coûts agrégés à la demande CSSF RTS

Possible création d'une plateforme unique de l'Union pour la notification des incidents (long terme)

Pilier II – Gestion, classification et notification des incidents TIC

Résumé et questions pratiques

Les prochaines étapes à accomplir

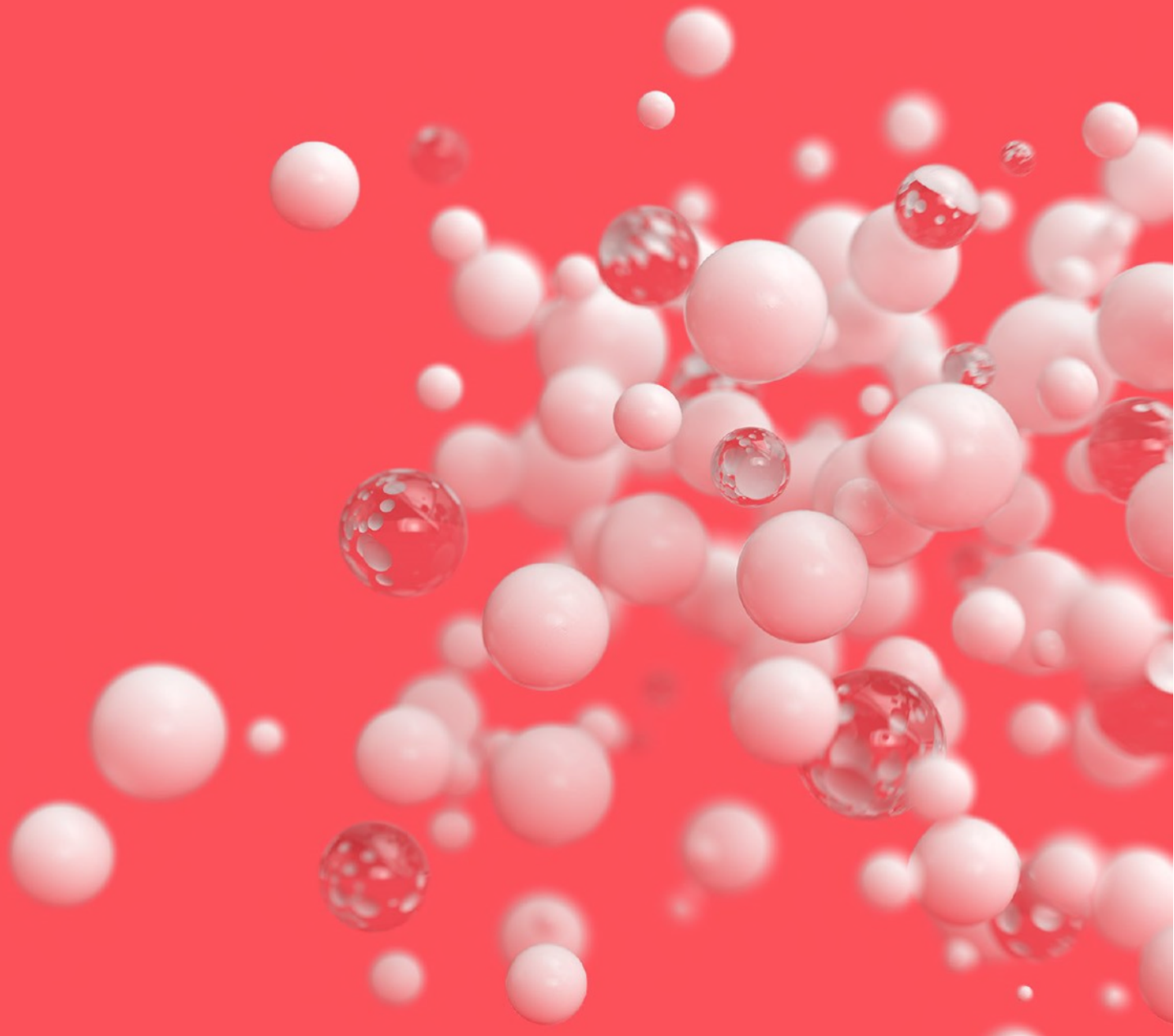
- Mise à jour des procedures de notification (délais)
- Mise en place d'une chaîne interne de reporting
- Création d'une fonction dediée (communication)

Quelques questions pratiques

- Si je suis une entité soumise à NIS2, quel formulaire utiliser?
- Comment gérer la notification des incidents survenus auprès d'un prestataire de service TIC?
- Puis-je déléguer la notification des incidents?

Pilier III

Test de résilience opérationnelle numérique



Pilier III – Test de résilience opérationnelle numérique

- Tests appropriés pour toutes les entités financières :
  - Programme de test
  - Principe de proportionalité
    - ➢ fonctions critiques ou importantes : 1 fois par an

- Test avancés de pénétration fondés sur la menace :
  - o Entités identifiées par l'autorité compétente
  - o Tous les 3 ans (autorité compétente peut augmenter ou réduire fréquence)
  - o Porte sur les fonctions critiques ou importantes
  - o Validation du plan (y compris étendue des fonctions testées) par l'autorité compétente
  - o Rapport d'audit

Pilier III – Test de résilience opérationnelle numérique

Résumé et questions pratiques

Les prochaines étapes à accomplir

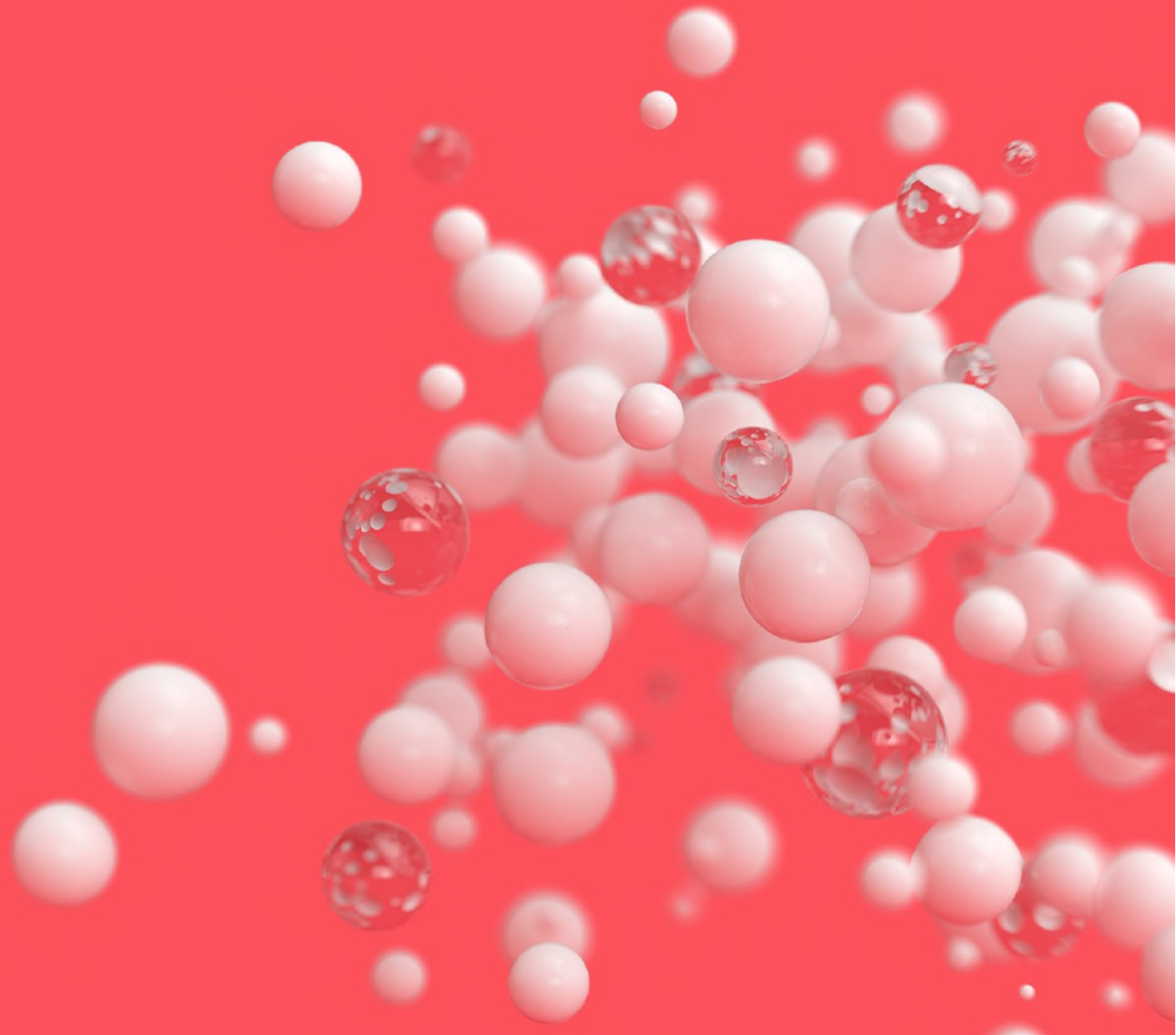
- Identifier les fonctions critiques et importantes
- Mise à jour des procédures de test existantes
- En cas d'identification par la CSSF, identifier les CIF soumises à des tests avancés, mise en place des protocoles de test

Quelques questions pratiques

- Faut-il adapter le cadre TIBER- EU?
- Faut-il intégrer les prestataires tiers dans l'exécution des tests?

Pilier IV

Gestion des risques liés aux prestataires de services TIC



Pilier IV – Gestion des prestataires TIC

- Entités financières restent responsables

- Stratégie du risque lié aux prestataires tiers de services
  - Ecrit
  - Inclut une politique relative aux fonctions critiques ou importantes
  - Identification des risques de concentration et dépendance
  - Approche au niveau du groupe autorisée
  - Revue obligatoire par l'organe de direction
  - Distribution des responsabilités (cycle de vie du contrat)

Pilier IV – Gestion des prestataires TIC

- Registre d'informations
  - Liste de tous les accords contractuels TIC
  - Identification des contrats qui couvrent des CIF
  - Focus sur les sous-contractants de CIF
  - Identification des contrats intra-groupe
  - Supervision : notification 1x / an

A préparer pour le 17 janvier 2025

Pilier IV – Gestion des prestataires TIC

- Avant de conclure un accord :
  - Informer l'autorité competente de "tout projet" d'accord portant sur une CIF
  - Due diligence : évaluation préliminaire du prestataire (inclu intra-groupe)
  - Analyse de risque au niveau de l'entité et/ou du groupe
  - CIF analyse du risque liée à l'externalisation du TIC
- Chaîne de sous-traitance d'une CIF : quel niveau de contrôle?

  CIF : contrôle complet de la chaîne de sous-traitance

Pilier IV – Gestion des prestataires TIC

- Dispositions contractuelles (art. 30)
  - Description claire des services
  - CIF : Sous-traitance autorisée ou non + conditions
    Localisation des services ; lieux de stockage (y compris du ST)
  - Protection des données (y compris données personnelles)
  - Récupération des données en cas d'insolvabilité, de résolution, de cessation des activités par le PS
  - Description des niveaux de services
  - Obligation pour le PS de fournir une assistance en cas d'incident
  - Obligation pour le PS de coopérer avec les autorités
  - Droits de résiliation
  - Implication du PS dans les formations de sensibilisation

CIF

- Description complète des niveaux de services (indicateurs qualité, mesures correctives)
- Obligation de notification des développements
- Obligation du PS de mettre en oeuvre et de tester des plans d'urgence
- Obligation du PS de participer au test de pénétration fondé sur la menace
- Droit d'assurer un suivi des performances : Droit "illimité" d'accès, d'inspection et d'audit
- Stratégie de sortie incluant une période de transition adéquate obligatoire

Clauses contractuelles types?

Pilier IV – Gestion des prestataires TIC

RTS sur la stratégie d'externalisation

POLICY ISSUE 1: DEFINITION OF CRITICAL AND IMPORTANT FUNCTIONS

Options considered

12. Option A: relying on the definition provided under DORA but providing more detailed criteria regarding the notion of "critical and important functions".

13. Option B: Referring to definition of DORA only as the draft RTS is about the content of the policy.

Cost-benefit analysis

14. Specifications to the definition would lead to a higher level of harmonization. However, a too specific definition would create the risk that it leaves out some aspects that might become more relevant over time. In addition, considering the different types of financial entities that are subject to DORA, relying on the definition within DORA, without the provision of detailed specifications seems to be more appropriate.

Preferred option

15. Option B has been retained.

Pilier IV – Supervision de certains prestataires « critiques »

- Prestataires TIC qui sont “critiques” pour les entités financières en fonction de leur importance systémique
- Désignés par les AES (liste)
- Prestataires tiers critique établi en dehors UE doit établir une filiale dans l’Union

- Superviseur principal : Supervise les conditions de sécurité liées aux services prestés et le risque pour les entités financières
- Coordination entre les autorités de supervision

Pilier IV – Gestion des prestataires TIC

Résumé et questions pratiques

Les prochaines étapes à accomplir

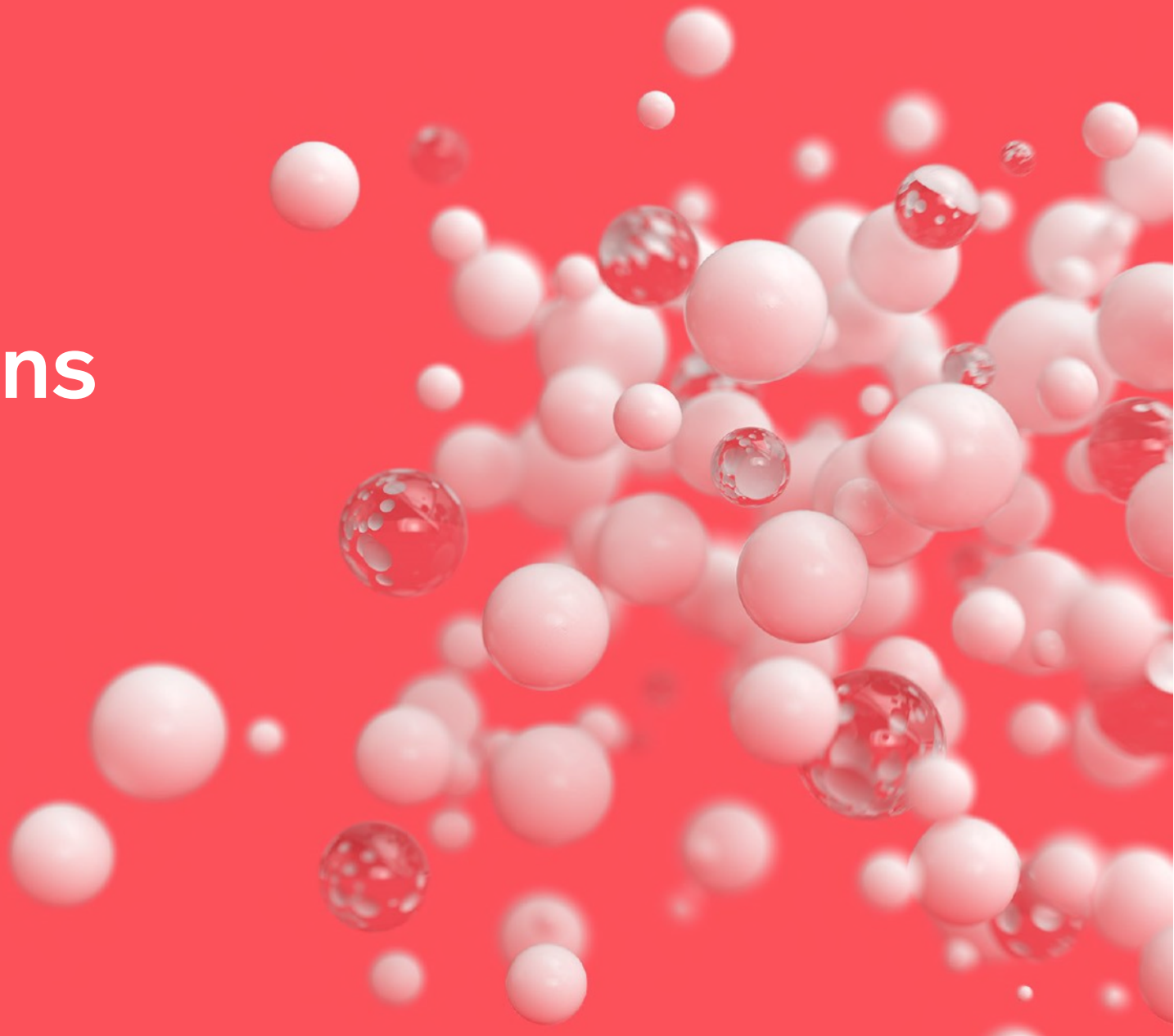
- Gap analysis des contrats existants
- Registre d'information
- Négociations avec prestataires tiers

Quelques questions pratiques

- DORA a-t-il le même champ d'application que la circulaire CSSF 22/806?
- Les prestataires TIC intra-groupe sont-ils dans le champ d'application de DORA ?
- Les prestataires TIC établis hors EU sont-ils visés par DORA ?

Pilier V

Partage d’informations

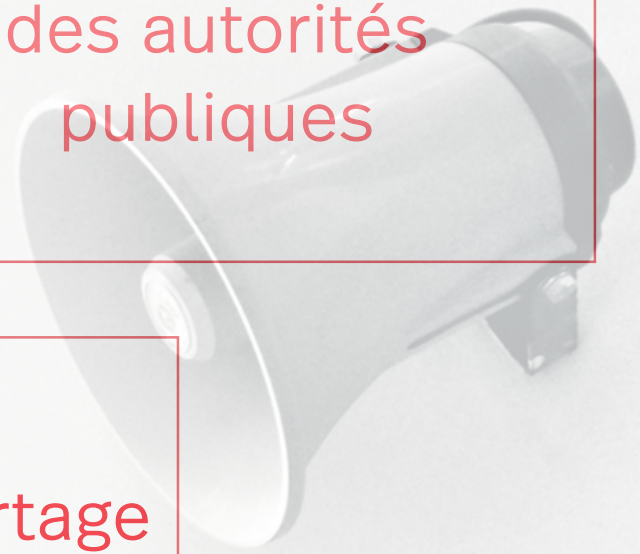


Pilier V – Partage d'informations

Partage d'informations entre entités financières notamment sur les cybermenaces

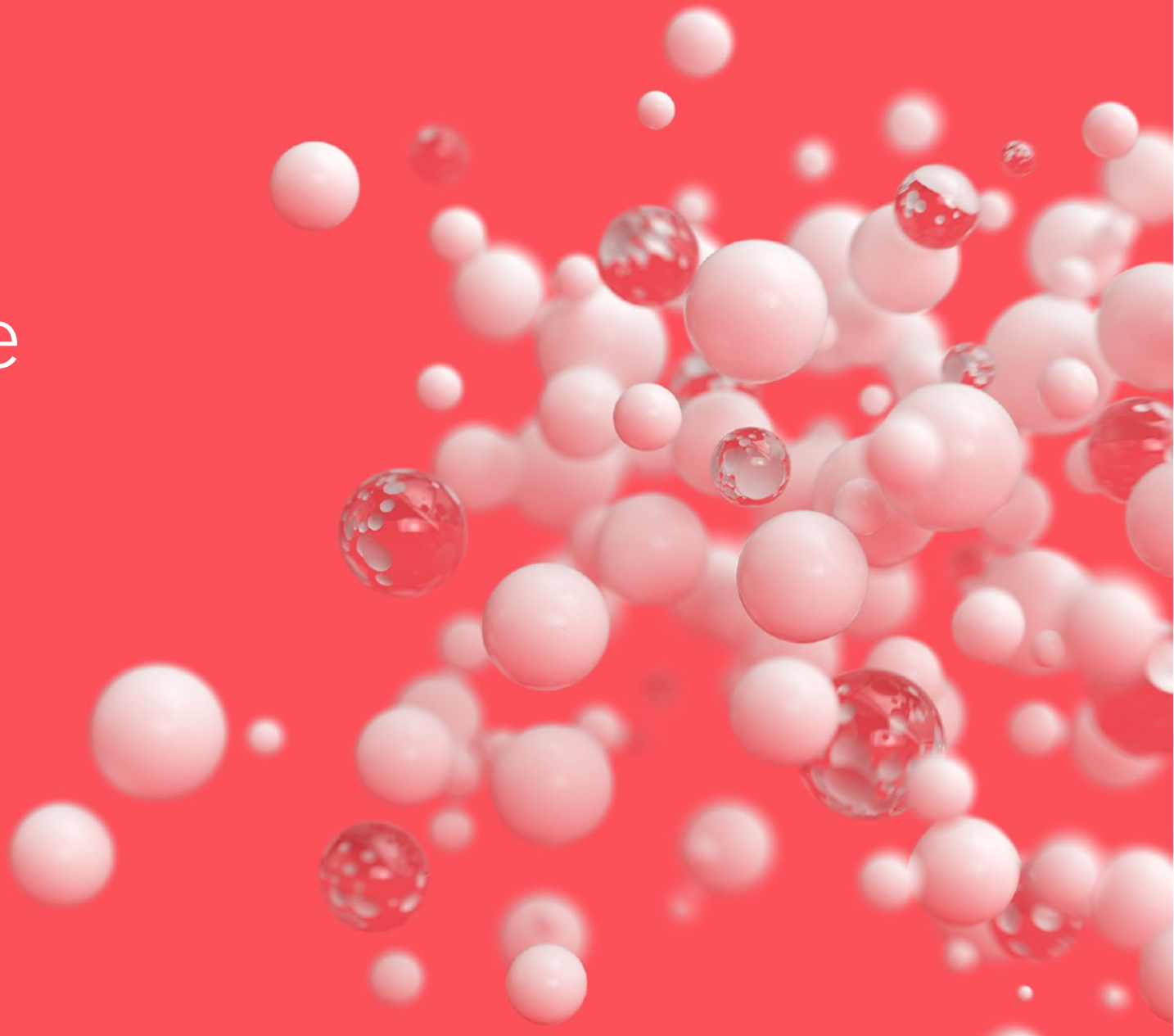
Possible participation des autorités publiques

Dispositifs de partage d'information



Supervision et Sanctions

Focus sur le projet de loi luxembourgeois n°8291



Projet de loi luxembourgeois n°8291

- <u>Calendrier</u>

➢ 04 août 2023 – dépôt du Projet de loi à la chambre des députés

➢ 07 mai 2024 – avis complémentaire du Conseil d'Etat

- <u>Quels sont les objets du projet de loi</u> ?

(i) désigner les autorités compétentes au Luxembourg chargées de veiller à l'application du Règlement DORA par les personnes soumises à leur surveillance (à savoir, la Commission de surveillance du secteur financier et le Commissariat aux assurances) ;

(ii) à doter lesdites autorités compétentes de pouvoir de surveillance et d'enquête nécessaires à l'exercice de leurs fonctions ;

(iii) À établir un régime de sanctions et d'autres mesures administratives notamment une amende administrative d'un montant maximal pouvant aller jusqu'à 5.000.000 euros, telle que prévue par le Projet tant pour les personnes morales que pour les personnes physiques.

DORA : quelles priorités?

- Identification des fonctions métier et des fonctions critiques et importantes (définition)
- Registre des informations : 17 Janvier 2025 !!
- Revue des contrats portant sur des CIF (Gap analysis)
- Définition du cadre de gestion du risque (stratégie de resilience; stratégie de sous-traitance)
- Revue des plans, procedures existantes ; adaptation du plan de notification des incidents

Q&A

Contact

Camille Saettel
Counsel, Digital Business
T +352 26 21 16 38
M + 352 691 166 751
camille.saettel@simmons-simmons.com

Maya Coumes
Supervising Associate, Regulatory
T +352 26 21 16 59
M + 352 691 116 67 53
maya.coumes@simmons-simmons.com

simmons-simmons.com

STRICTLY PRIVATE AND CONFIDENTIAL