BANQUE DE FRANCE
EUROSYSTÈME

PÔLE
STABILITÉ
FINANCIÈRE

ACPR
BANQUE DE FRANCE

LE RÈGLEMENT DORA : UNE NOUVELLE LÉGISLATION FACE AUX RISQUES CYBER

YANN MARIN/AZIZA HALILEM
DIRECTION DES AFFAIRES INTERNATIONALES

BANQUE DE FRANCE
EUROSYSTÈME

PÔLE
STABILITÉ
FINANCIÈRE

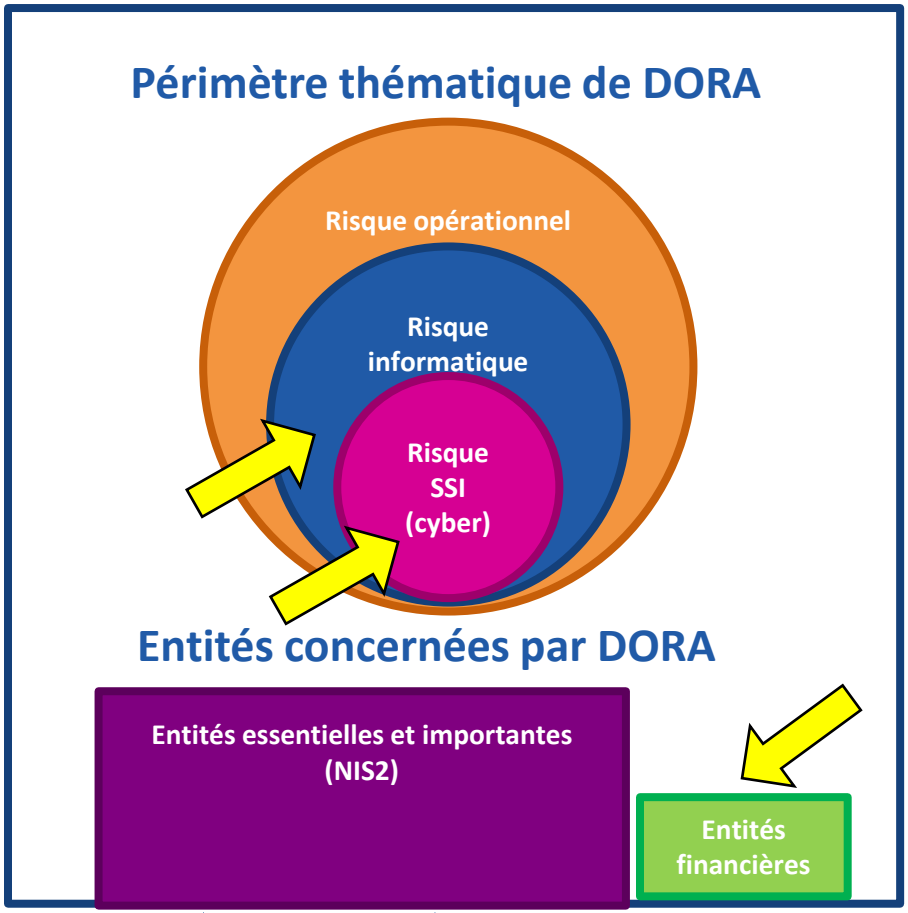
ACPR
BANQUE DE FRANCE

DORA, UN NOUVEAU CADRE COHÉRENT ET EXIGEANT POUR L'ENSEMBLE DU SECTEUR FINANCIER

Sommaire

OBJECTIFS ET PÉRIMÈTRE DE DORA

DORA renforce le **versant numérique de la résilience opérationnelle** du secteur financier par des mesures portant sur la sécurité des réseaux et des systèmes d'information



- Des règles pour **l'ensemble du secteur financier (lex specialis par rapport à NIS)**
  - Secteur bancaire au sens large (EC, EI, EP, EME…).
  - Organismes d'assurance,
  - Infrastructures et acteurs des marchés financiers,
  - Et aux marges du secteur financier :
    - Intermédiaires d'assurance,
    - Services de communication de données financières,
    - Agences de notation…

LES ATTENTES POUR LA SUPERVISION

Intégration au plus haut niveau des considérations liées aux TICs. Des plans de rétablissement plus élaborés en intégrant la substituabilité des services.

Amélioration du capital humain des Entités financières : dispositif de formation à destination des membres de l'organe de direction et actions de sensibilisation.

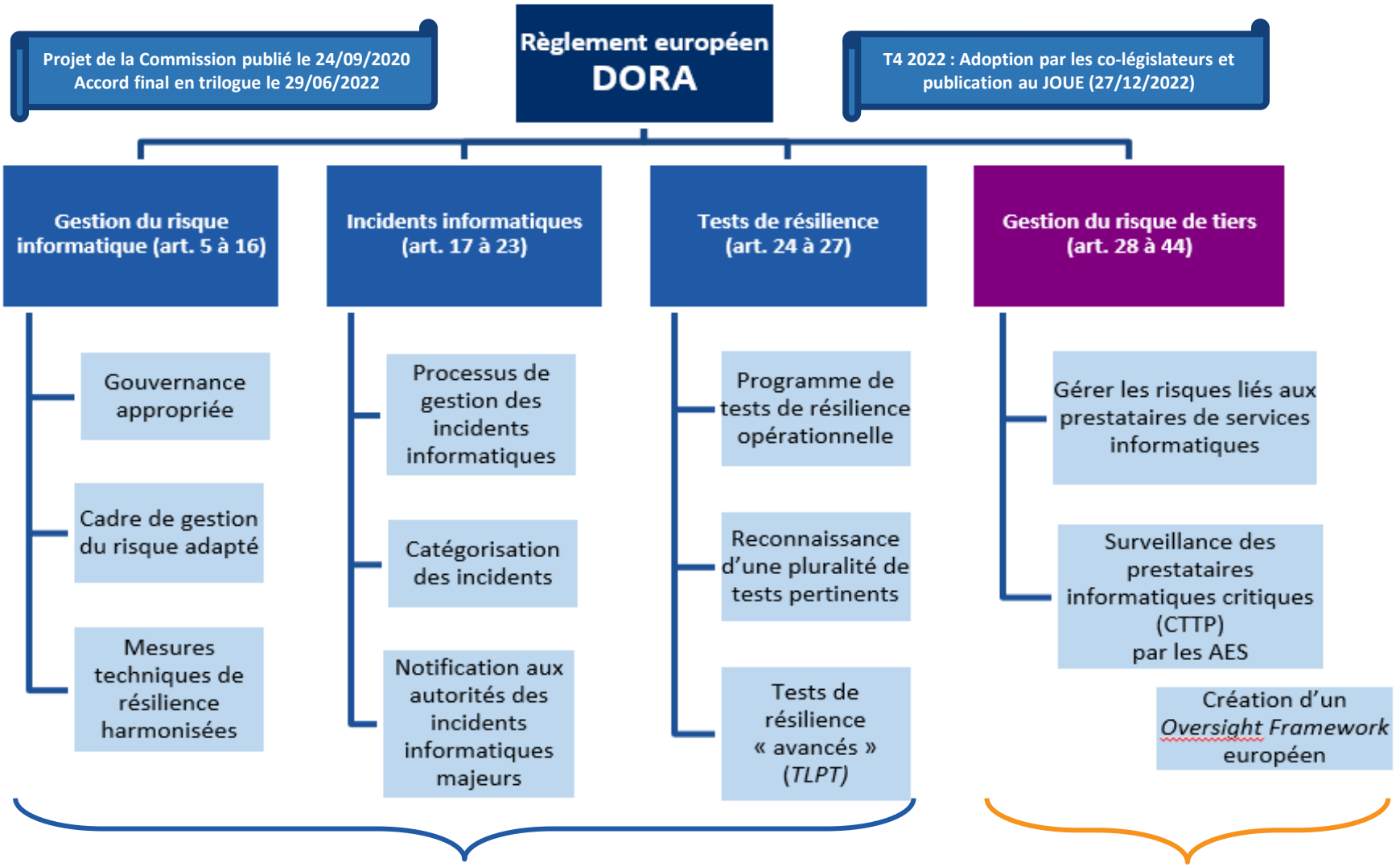
Renforcement du cadre réglementaire de la gestion du risque opérationnel

Signalement des incidents : un signalement plus harmonisé selon des formats standardisés. Une vision plus élargie des vulnérabilités côté supervision.

Tests de résilience opérationnelle numérique à l'échelle européenne : Optimisation des coûts et reconnaissance transfrontalière des tests (Europe).

Risques pour les tiers liés aux TIC : le cadre de surveillance des tiers donnera plus de sécurité juridique, un niveau d'assurance sur la sécurité des actifs contenus dans le Cloud et une meilleure confiance vis-à-vis de ces acteurs.

PERSPECTIVES RÉGLEMENTAIRES
PRÉSENTATION SYNTHÉTIQUE

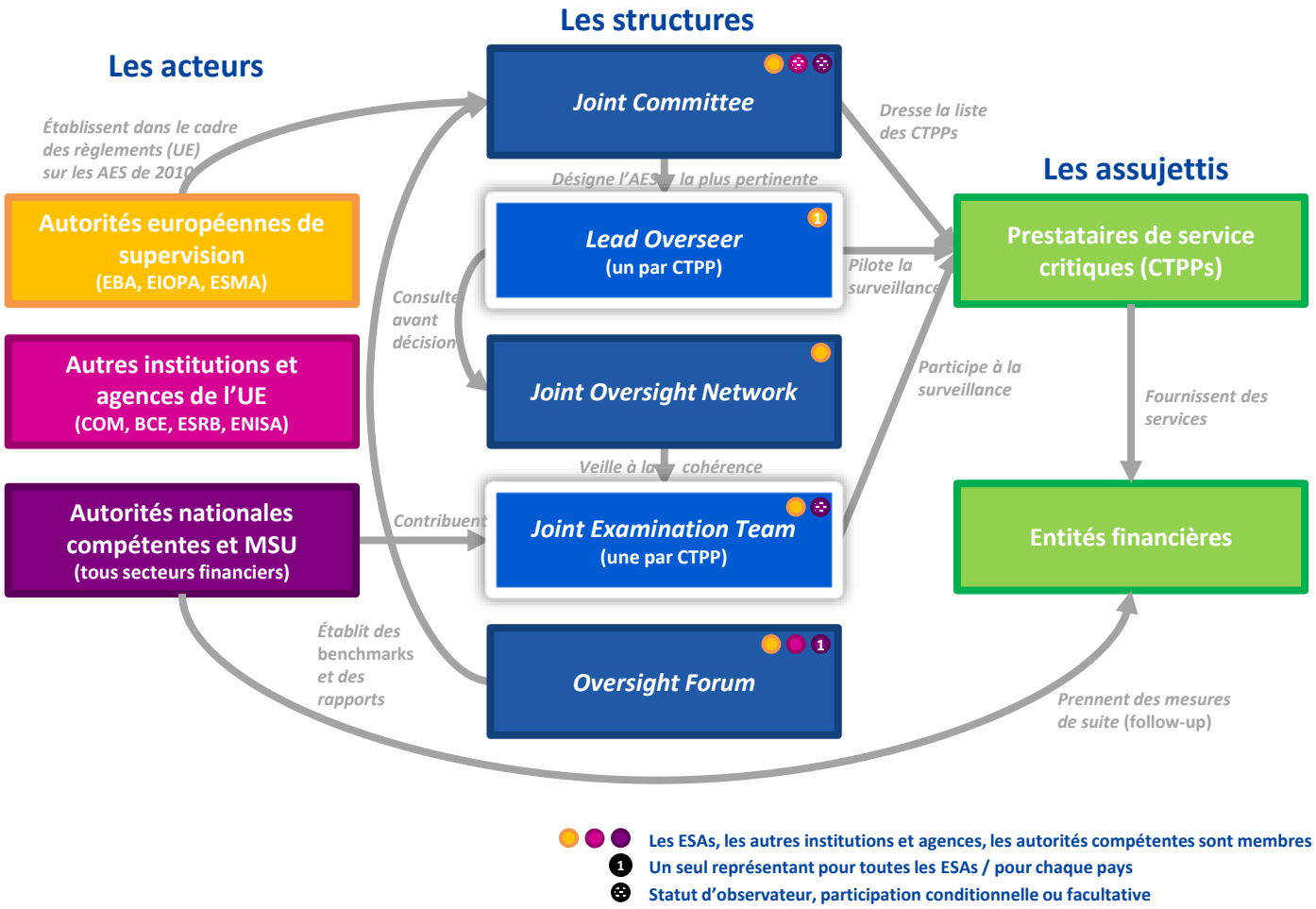


FOCUS PARTICULIER : ÉLÉMENTS À RETENIR POUR LA GESTION DU RISQUE DE TIERS

- Ne pas confondre les cadres et les acteurs…

	Renforcement du cadre de supervision	Création du cadre de surveillance
Superviseur	Les autorités compétentes (la BCE + les ANC)	Le superviseur principal (une des 3 AES), assisté d'une équipe conjointe (ANC, experts)
Assujetti	Les entités financières	Les prestataires informatiques critiques
Risques	Risque TIC + risque de tiers (y compris le risque de concentration)	Risque TIC (y compris celui soulevé par les sous-contractants)
Pouvoirs	Contrôle sur pièce et sur place. Demande d'info, documents stratégiques, tests…	Demandes d'info, enquêtes générales, inspections, recommandations et astreintes.

FOCUS SUR LE CADRE DE SURVEILLANCE DIRECTE DES PRESTATAIRES CRITIQUES



APPORTS DE DORA À LA SURVEILLANCE DES TIERS

Aucun des principes introduits par DORA n'est inédit

- L'entité financière reste la responsable du risque
- Le risque doit être géré de manière proportionnelle
- Les entités financières doivent établir une stratégie relative au risque de tiers
- Les entités financières doivent maintenir un registre d'information et signaler au superviseur lorsqu'un contrat porte sur des fonctions critiques ou importantes
- Évaluation du risque préalablement à la signature du contrat, sécurité et accès aux données et stratégies de sortie

Les bonnes pratiques contractuelles sont réaffirmées

- Clarté des obligations réciproques
- Accords de niveau de service
- Clauses de réversibilité…

Mais DORA harmonise des termes, des périmètres et des pratiques

- « risque de tiers » plutôt qu'« externalisation»
- Une approche commune partagée avec les filiales et concurrents français et européens, des secteurs de la banque et de l'assurance…

DORA apporte une réponse au déséquilibre existant dans les relations entre entités/tiers.

EN FIN DE COMPTE, DORA PROMEUT UNE DEMARCHE CONSTRUCTIVE

- **Un objectif de clarification**
  - Harmonisation des normes mais pas de révolution des pratiques
- **DORA reflète une priorité croissante du risque cyber pour le législateur comme pour les superviseurs**
  - Une singularité qui justifie une harmonisation entre secteurs
  - Des outils de gouvernance dédiés
  - Un *reporting* particulier
- **DORA promeut une relation de confiance avec les autorités**
  - *Reporting* volontaire des menaces
  - Encouragement à utiliser des clauses contractuelles standard (lorsqu'elles existent)
  - Une réduction des risques de tiers pour les entités financières grâce à la surveillance des prestataires critiques par les AES et les superviseurs
  - Échanges d'information entre entités financières et en y associant les autorités

DES ENJEUX ESSENTIELS POUR L'ACPR

2022-2024 : Participer aux travaux sur les textes de niveau 2

- DORA attribue 13 mandats aux AES à remplir d'ici à la mi-2023 : un défi collectif pour les autorités européennes et nationales
- Les autorités nationales de supervision ont une expertise à faire valoir
- L'ACPR souhaite promouvoir l'efficacité et la qualité de la gouvernance et éviter le formalisme

D'ici à 2025 : Préparer la mise en œuvre de DORA avec les AES et le MSU

- Renforcer les compétences dans le domaine cyber qui restera une
- priorité stratégique pour les activités de contrôle de l'ACPR
- Être prêt à contribuer à la surveillance des prestataires critiques
- Mettre en place les nouveaux *reportings*

BANQUE DE FRANCE
EUROSYSTÈME

PÔLE
STABILITÉ
FINANCIÈRE

ACPR
BANQUE DE FRANCE

ANTICIPER L'ENTRÉE EN APPLICATION DE DORA

NOS ACTIONS DE SUPERVISION SE POURSUIVENT

- Orientations sectorielles EIOPA/EBA
- Notices ACPR
- Révision en 2021 de l'arrêté du 3/11/2014

Les enquêtes et restitutions régulières au marché permettent aux entités financières de s'améliorer

- Restitution des enquêtes
- Appréciation de la maturité du secteur

Les inspections identifient les manquements des EF en matière de sécurité de l'information

- Contrôles sur place
- Restitution individuelle

Actions en vue de la préparation en cas de crise cyber

- Groupe de place Robustesse
- Protocole de gestion de crise cyber et Reporting pour les LSI et les organismes d'assurance

LES INSTITUTIONS FINANCIERES PEUVENT ET DOIVENT SE PRÉPARER

- **En anticipation de DORA, renforcer la gouvernance actuelle** est la meilleure préparation.
  - **Pas de changement de l'esprit de la règlementation** même si les exigences sont plus précises (risque de tiers) ou approfondies (TLPT)
- **Tirer les leçons des expériences pilotes** de registre des prestataires, de la détection et du *reporting* des incidents ou des tests d'intrusion « maison ».
- **Viser la *résilience* opérationnelle et non la seule maîtrise du *risque* opérationnel.**
- **Passer en revue les clauses de ses contrats de prestation TIC.**