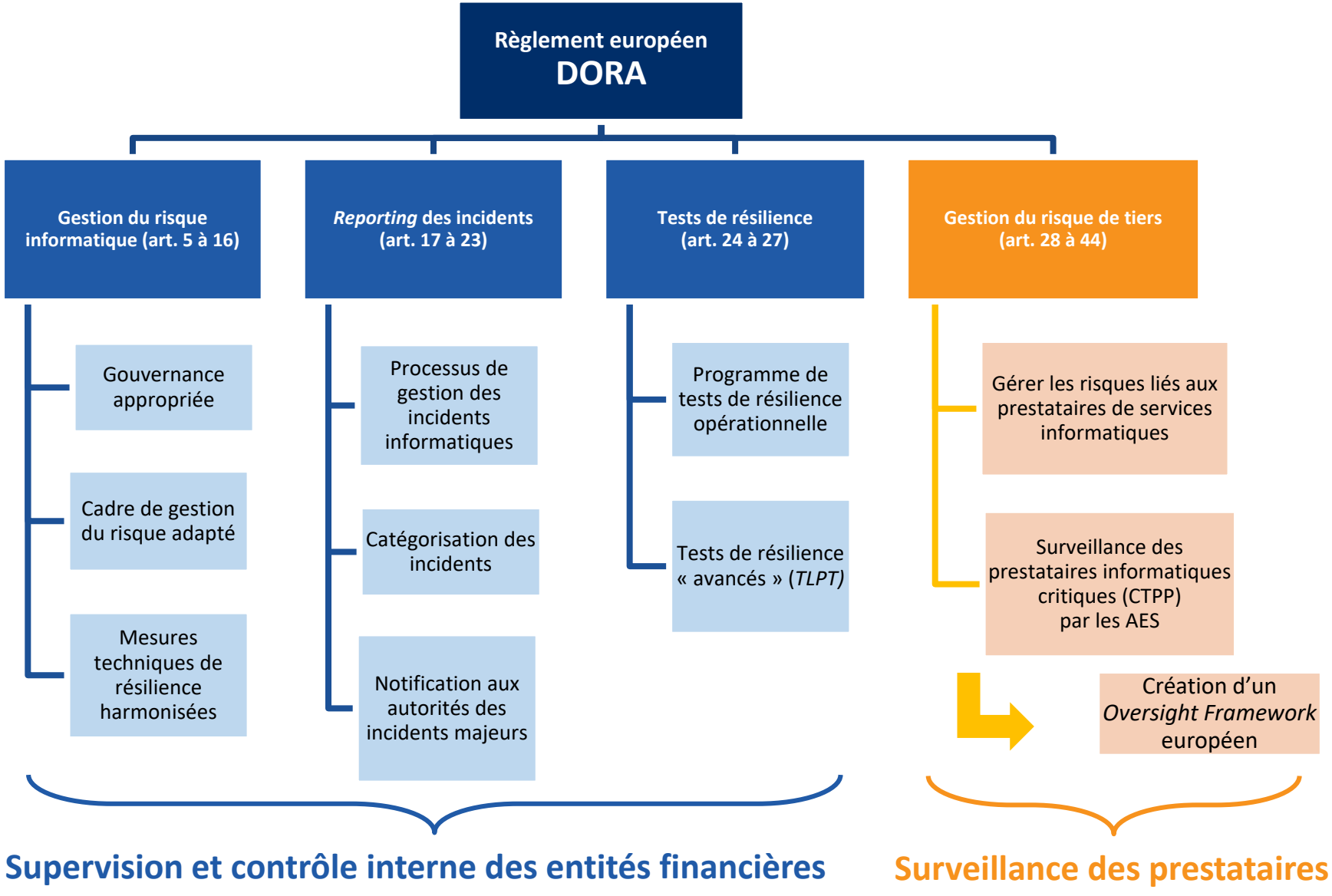
RÉUNION DE PLACE DORA

Introduction par Évelyne MASSÉ
Première Secrétaire générale adjointe

9 OCTOBRE 2024


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

SOMMAIRE

1. UN CADRE RÉGLEMENTAIRE VISANT À ASSURER LA RÉSILIENCE DU SECTEUR FINANCIER FACE AUX RISQUES LIÉS AUX TIC

PROPOS INTRODUCTIF

- DORA : un règlement, une directive, 9 RTS, 2 ITS, 2 *guidelines* et un *call for advice*

- Via un champ d'application particulièrement large, DORA met fin à la fragmentation actuelle (sectorielle), à certaines lacunes dans la règlementation voire à une absence de réglementation

- Entrée en application : 17 janvier 2025

- 3 notions au cœur de DORA :
  - La résilience opérationnelle numérique qui va au-delà de la sécurité des systèmes d'information
  - Les fonctions critiques ou importantes :
    - Art3(22) : « une fonction dont la perturbation est susceptible de nuire sérieusement à la performance financière d'une entité financière, ou à la solidité ou à la continuité de ses services et activités, ou une interruption, une anomalie ou une défaillance de l'exécution de cette fonction est susceptible de nuire sérieusement à la capacité d'une entité financière de respecter en permanence les conditions et obligations de son agrément, ou ses autres obligations découlant des dispositions applicables du droit relatif aux services financiers »
    - Il appartient aux entités financières d'établir des critères de criticité tout en s'assurant que les évaluations restent appropriées et proportionnées à leurs spécificités
  - La proportionnalité (article 4 de DORA)

- Le règlement ne se concentre pas uniquement sur la conformité aux exigences réglementaires

ACPR
BANQUE DE FRANCE

SOMMAIRE

1. ACTEURS ET CHAMPS DE COMPÉTENCE

<table>
<tr><th>Compétence ACPR
– secteur assurance</th><th>Compétence ACPR
– secteur bancaire</th><th>Compétence AMF</th><th>Compétence Banque de France</th></tr>
<tr><td>Organismes d’assurance et de réassurance (sauf les organismes écartés du périmètre de Solvabilité II en raison de leur taille)</td><td colspan="3">Contrepartie centrale</td></tr>
<tr><td>Intermédiaires d’assurance et de réassurance et intermédiaires d’assurance à titre accessoire (sauf si micro-entreprises ou PME, cf. seuils fixés par DORA)</td><td>Établissements de crédit
(pour les compétences ne relevant pas de la BCE au titre du MSU)</td><td colspan="2">Dépositaires centraux de titres</td></tr>
<tr><td rowspan="2">Institutions de retraite professionnelle (sauf < à 15 adhérents)</td><td>Entreprises d’investissement
(sauf si exemptées à l’article 2 ou 3 de MiFID)</td><td>Sociétés de gestion</td><td rowspan="6"></td></tr>
<tr><td colspan="2">Plateformes de négociation
(MR, OTF, MTF)</td></tr>
<tr><td rowspan="5"></td><td>Établissements de monnaie électronique</td><td>Gestionnaires de fonds d’investissement alternatifs
(sauf petits & moyens)</td></tr>
<tr><td>Établissements de paiement</td><td rowspan="2">Prestataires de services de financement participatif</td></tr>
<tr><td>Prestataires de services d’information sur les comptes</td></tr>
<tr><td colspan="2">Prestataires de services sur crypto-actifs
Émetteurs de jetons se référant à des actifs (ART)</td></tr>
</table>

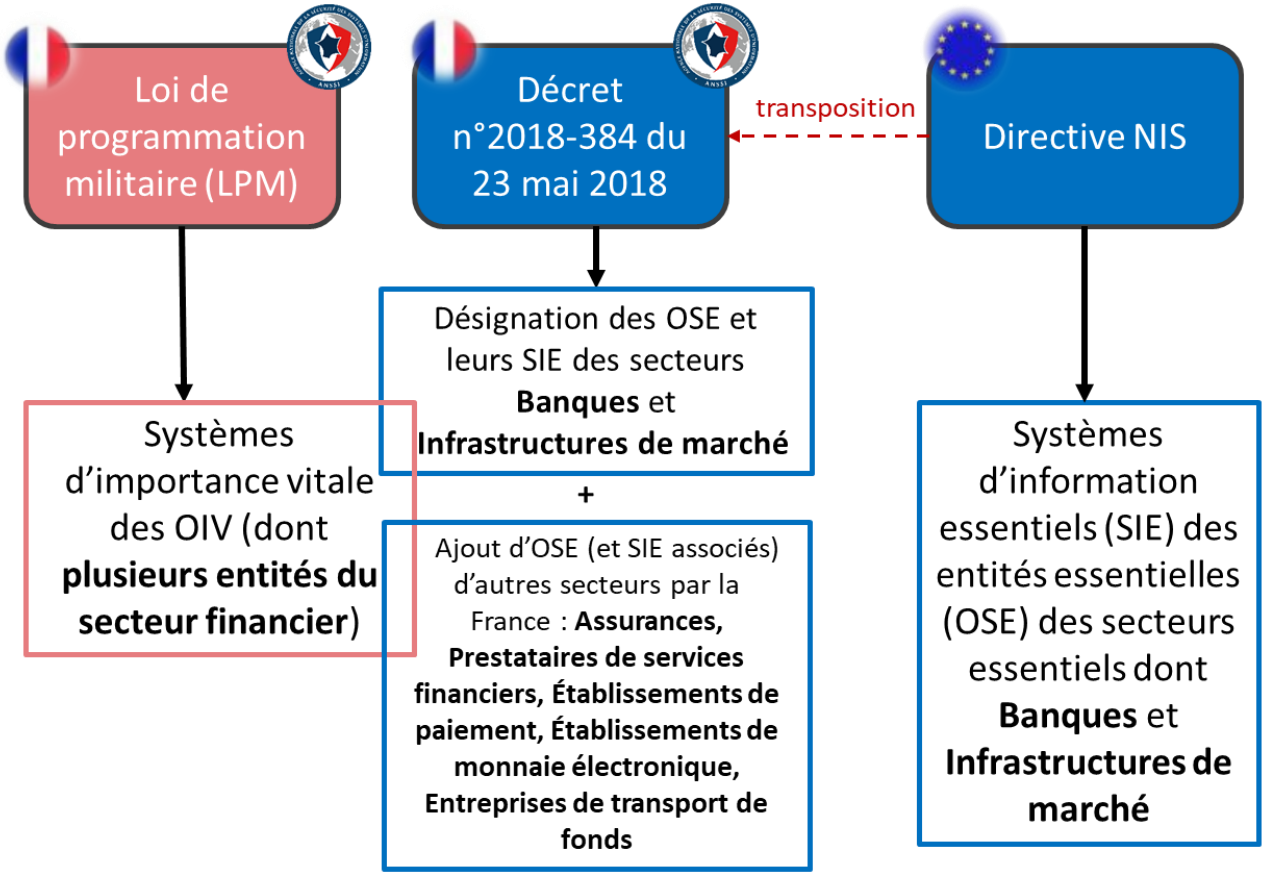
2. ARTICULATION AVEC LES ORIENTATIONS PRÉEXISTANTES

- **Orientations des autorités européennes de supervision sur la gestion du risque informatique** et/ou *Cloud*
  - En cours de réflexion

- **Orientations EBA sur la gestion du risque de sous-traitance** (2019)
  - Remplacées par le volet *risque de tiers* de DORA en ce qui concerne les prestataires externes de services informatiques.

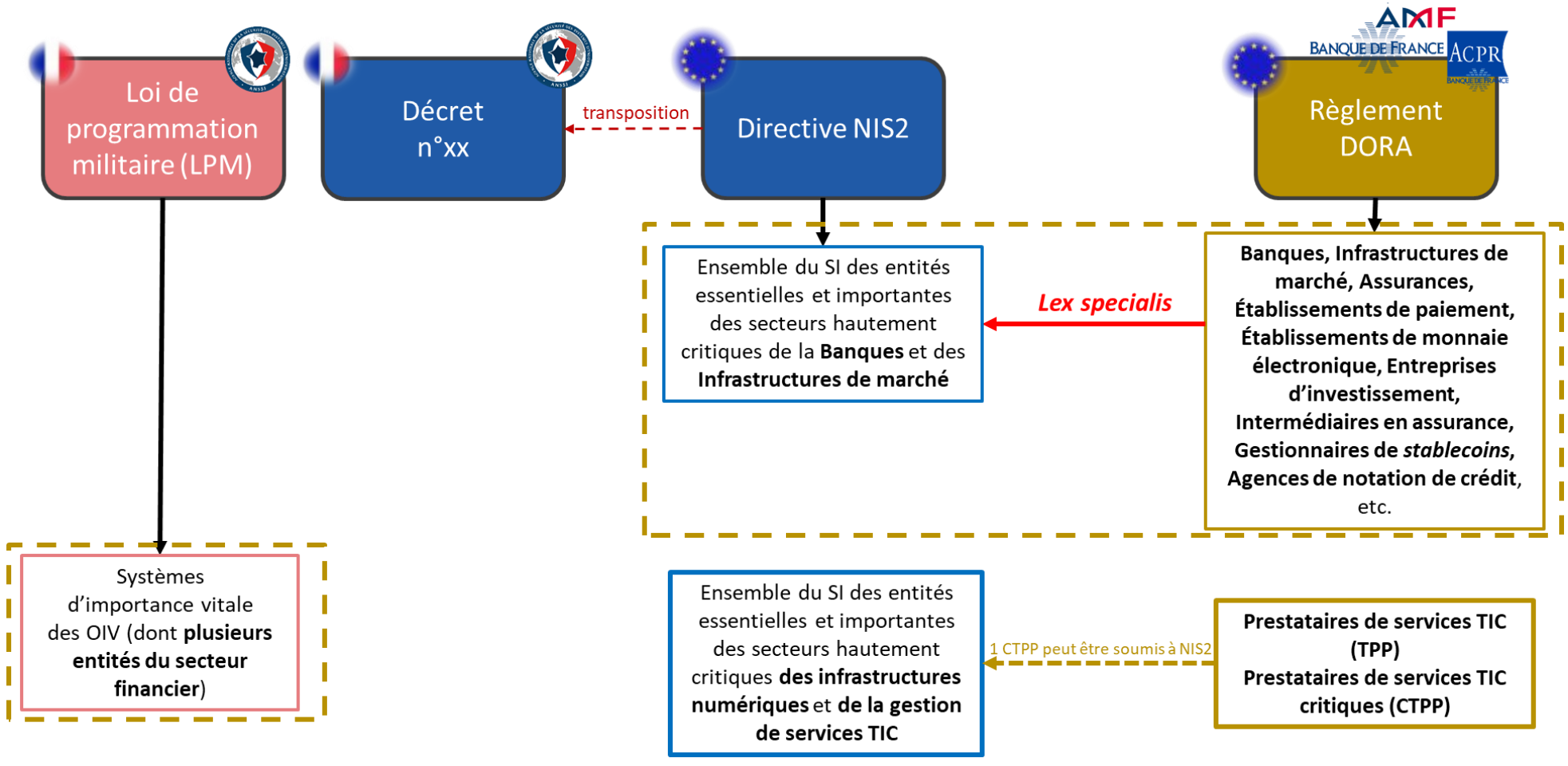
3. ARTICULATION AVEC LA DIRECTIVE NIS2

Avant DORA

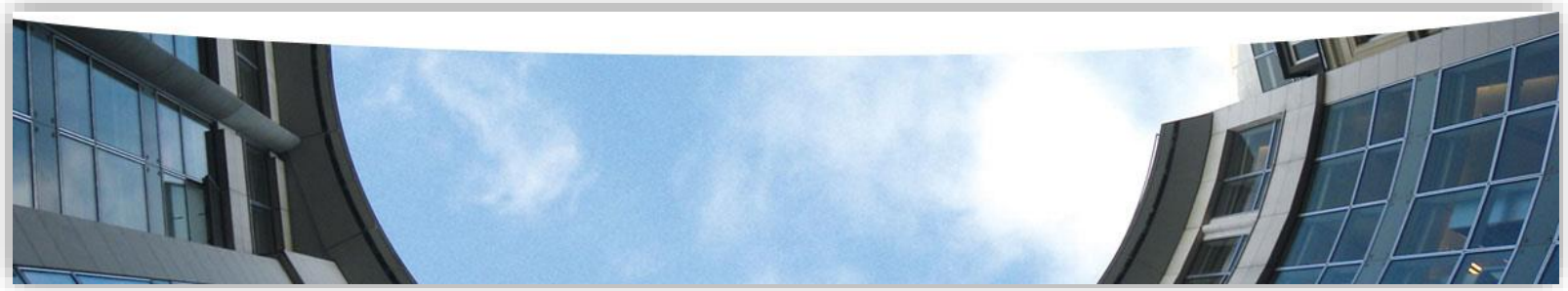


3. ARTICULATION AVEC LA DIRECTIVE NIS2

Avec DORA



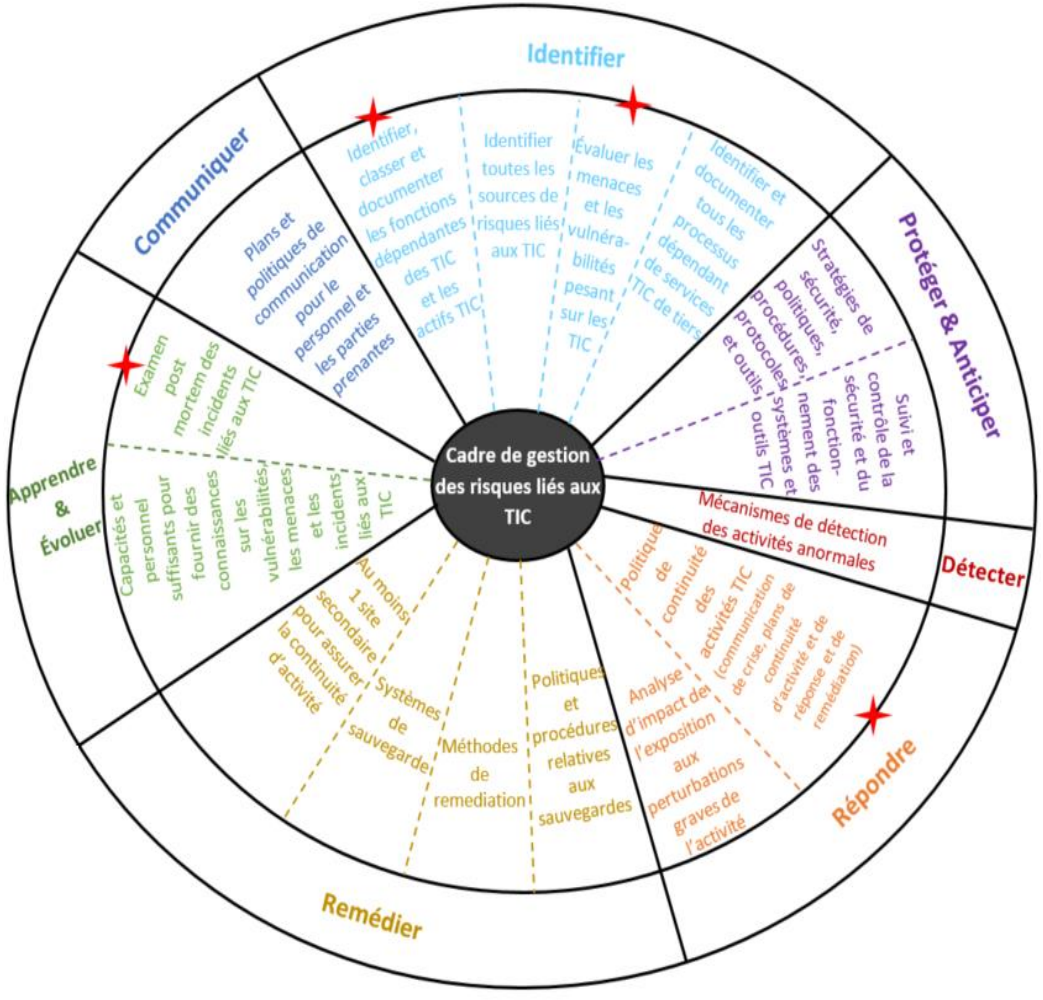
AVEZ-VOUS DES QUESTIONS ?



2. UNE GOUVERNANCE, UN CADRE DE GESTION DES RISQUES ET DE TESTS RENFORCÉS

SOMMAIRE

1. CADRE DE GESTION DES RISQUES LIÉS AUX TIC
A. STRUCTURE GLOBALE



- DORA définit un cadre de gestion des risques à destination de l'ensemble des entités financières, et un régime simplifié à l'égard d'un nombre limité d'entités
- Le cadre recouvre les dispositions contenues dans le Règlement et le RTS *Risk Management Framework* (RMF)
- Importance de la phase d'identification : aboutir à une cartographie complète des services critiques et importants
- Proportionnalité : exigences globalement élevées mais adaptées à l'entité.

Viser la résilience opérationnelle et non la seule maîtrise du risque opérationnel

1. CADRE DE GESTION DES RISQUES LIÉS AUX TIC
B. CADRE FORMEL DE GESTION DES RISQUES

- Les entités financières soumises à DORA sont tenues de mettre en œuvre un **cadre formel** de gouvernance et de gestion des risques liés aux TIC
  - Documents, politiques écrites et procédures, outils et méthodes (déclinaison notamment du RTS RMF)
    - Politiques (notamment liées aux actifs informatiques, chiffrement, opérations, contrôle d'accès, etc.. et procédures (Gestion des capacités et des performances, sécurité des données, etc..)
    - Mesures de sécurité (journalisation, gestion de la sécurité des réseaux, sécurisation des informations en transit)
    - Gestion des projets et des modifications
    - Politiques de continuité des activités informatiques et plans de réponse et de rétablissement informatiques
  - Augmentation des livrables à traiter remis par les entités financières

ACPR
BANQUE DE FRANCE

2. TESTS DE RÉSILIENCE

- L'article 24 de DORA impose aux entités financières de son champ d'application la définition d'un **programme de tests de sécurité**
  - Selon une approche par les risques
  - Partie intégrante du cadre de gestion des risques
  - L'article 25 reconnait une pluralité de types de tests pertinents (scans, tests d'intrusion, etc.).
- Si des TLPT internes sont prévus dans le programme d'une entité elle-même soumise aux TLPT DORA, ils ne pourront les remplacer
- En effet, les TLPT deviendront une **obligation triennale pour une sélection d'établissements** dont la désignation, fondée sur les critères du RTS et sur le principe de proportionnalité, est à la main des autorités TLPT nationales (ACPR, BdF, AMF) et de la BCE pour les *Significant Institutions*
  - Ces établissements seront avertis de leur désignation à partir de l'entrée en application de DORA
  - La date de lancement du 1er TLPT sera quant à elle notifiée *via* une seconde lettre postérieure

→ Pour tout savoir sur les TLPT, un webinaire est organisé le 15 octobre par la TCT-FR

3. GESTION DU RISQUE DE TIERS
A. PRINCIPES GÉNÉRAUX

- Le règlement DORA aborde le **risque de tiers** selon deux volets :

  – Pour l'**entité financière** : la stratégie de gestion du risque lié aux prestataires de services aux Technologies de l'Information et de la Communication (TIC)

  – Pour les **prestataires critiques** de **services TIC** : un cadre de surveillance par les trois Autorités Européennes de Surveillance (AES)

  DORA confirme dans ses textes de niveau 1 et 2 :

  ✓ la **responsabilité ultime** de l'entité financière en cas d'externalisation

  ✓ l'obligation d'**enregistrer** tous les **contrats** de prestations TIC externalisés

  ✓ l'application d'un **cadre de gestion** du **risque d'externalisation** de service TIC portant sur des fonctions métier critiques ou importantes

  ✓ L'obligation de disposer d'une **stratégie** en matière de risques liés aux prestataires tiers de services TIC et une **politique** liée aux services TIC supportés par des tiers portant sur des fonctions critiques ou importantes

ACPR
BANQUE DE FRANCE

3. GESTION DU RISQUE DE TIERS

B. IDENTIFICATION DES PRESTATAIRES ET DES SERVICES INFORMATIQUES EXTERNALISÉS

- Obligation de maintenir à jour un **registre d'information** *(RoI)* sur base individuelle, sous-consolidée et consolidée
- Pour l'identification, les types de services TIC ont été listés dans l'annexe 3 de l'ITS sur le registre (version non définitive) :

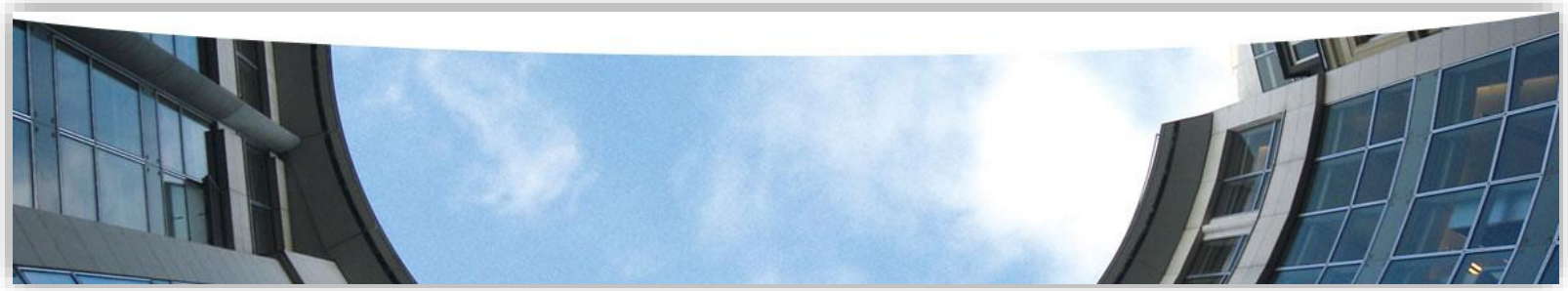
Type of ICT services
ICT project management
ICT development
ICT help desk and first level support
ICT security management services
Provision of data
Data analysis
ICT, facilities and hosting services (excluding Cloud services)
Computation
Non-Cloud data storage
Telecom carrier
Network infrastructure
Hardware and physical devices
Software licencing (excluding SaaS)
ICT operation management (including maintenance)
ICT consulting
ICT risk management
Cloud services : IaaS
Cloud services : PaaS
Cloud services : SaaS

3. GESTION DU RISQUE DE TIERS
C. CHAINE LIÉE A LA SOUS-TRAITANCE

- Des exigences supplémentaires s'ajoutent sur la maîtrise de la sous-délégation par le prestataire tiers
- Le RTS sur la sous-traitance de services portant sur des fonctions métiers critiques ou importantes aborde notamment les éléments suivants :
  - **Évaluation ex ante sur les caractéristiques des contrats**
    - Juridiction du sous-traitant de service TIC et de sa maison mère
    - Nombre de sous-traitants
    - Nature des données partagée avec les sous-traitants
    - Évaluation des impacts en cas de rupture/perturbation de la continuité de service
    - Risque de concentration
    - …
  - **Revue de conformité des clauses dans les contrats**
    - sur l'engagement des sous-traitants dans la continuité de service
    - sur l'accès à la documentation sur toute la chaîne
    - sur les droits d'audit
    - en cas de mise à jour en cas de modification de la chaîne de sous-traitance
    - de résolution du contrat
      - en cas de modification non validée par l'entité financière
      - en cas de sous-traitance unilatérale par le prestataire de service (rang 1)

- Revue des contrats en stock avec mise à jour des clauses
- Revue continue des contrats

AVEZ-VOUS DES QUESTIONS ?



3. LES REPORTINGS

SOMMAIRE

1. REPORTING DES INCIDENTS MAJEURS
A. INCIDENTS MAJEURS LIÉS AUX TIC

- Les entités financières doivent notifier à leur autorité compétente les incidents majeurs liés aux TIC.
  - Toutes les entités financières de son périmètre, *Significant Institutions* incluses, doivent transmettre leurs reporting d'incidents liés aux TIC majeurs à l'ACPR qui se chargera de la transmission aux AES et à la BCE
  - Les critères de classification d'un incident comme majeur sont prévus par le règlement délégué (UE) 2024/1772 de DORA

1. REPORTING DES INCIDENTS MAJEURS

A. INCIDENTS MAJEURS LIÉS AUX TIC

Services TIC ou réseaux et systèmes d'information qui soutiennent des fonctions critiques ou importantes affectés

OU

Services financiers qui requièrent une autorisation, un enregistrement ou qui sont supervisés par des autorités compétentes

OU

Accès réussi, malveillant et non autorisé au réseau et aux systèmes d'information de l'entité financière

Au moins 2 parmi :

① Clients, contreparties financières, transactions
Nombre de clients affectés > 10% ou à 100 000
Nombre de contreparties financières affectées > 30%
Nombre/montant de transactions affectées > 10% du nombre/montant quotidien moyen
② Impact réputationnel : média, plaintes, etc.
③ Durée incident > 24h ou indisponibilité service TIC soutenant fcts critiques/importantes > 2h
④ Impact dans au moins 2 États membres
⑤ Impact sur la disponibilité, l'authenticité, l'intégrité et la confidentialité des données qui a une incidence sur la mise en œuvre des objectifs commerciaux ou sur le respect des exigences réglementaires
⑥ Coût & pertes > 100K€

OU

Tout accès réussi, malveillant et non autorisé au réseau et aux systèmes d'information qui peut entraîner une perte de données

1. REPORTING DES INCIDENTS MAJEURS
A. INCIDENTS MAJEURS LIÉS AUX TIC

- La notification initiale doit se faire dans les **4 h** après classification de l'incident comme majeur et sous **24 h** après sa détection. Un rapport intermédiaire doit être envoyé au plus tard **72 h** après la notification initiale, puis le rapport final au plus tard **1 mois** après le dernier rapport intermédiaire
- L'incident majeur est considéré comme résolu quand le service affecté revient à la normale. La durée de l'incident n'inclut pas le *problem management,* (analyse des causes, mise en œuvre de mesures correctrices et Retex)

1. REPORTING DES INCIDENTS MAJEURS
B. INCIDENTS MAJEURS LIÉS AUX PAIEMENTS

- La notification des incidents majeurs liés aux paiements, actuellement régie par la DSP2, fait désormais partie du champ de DORA et devra s'effectuer dans les mêmes conditions
- Mais, les critères de classification comme majeur d'un incident lié aux paiements sont toujours définis dans les Orientations EBA 2021/03
- **Les rapports d'incident majeur lié aux paiements devront être envoyés à l'ACPR, qu'il s'agisse d'un incident opérationnel ou de sécurité**
- La transposition en droit français des modalités de reporting est en cours

1. REPORTING DES INCIDENTS MAJEURS
C. CYBER-MENACES IMPORTANTES

- Le reporting des cyber-menaces importantes se fait sur la base du **volontariat** (alignement avec l'article 30 de la Directive NIS2) et du template prévu par DORA
- Le caractère volontaire du reporting des cyber-menaces pourra être réexaminé lors de la revue de DORA d'ici à janvier 2028, cf. art. 58(1)(b)
- Par ce reporting, les établissements peuvent contribuer à la résilience du secteur financier national/UE aux cyberattaques :
  - En assurant une meilleure connaissance du paysage des cyber-menaces au superviseur
  - En lui permettant de faire des recoupements avec d'autres menaces ou incidents cyber majeurs notifies par d'autres établissements
  - Dans certains cas, en lui permettant d'alerter les membres du Groupe de Place Robustesse, du protocole de gestion de crise cyber ACPR

1. REPORTING DES INCIDENTS MAJEURS
D. MODALITÉS DE TRANSMISSION

- Pour toutes les entités assujetties (ACPR et BCE):
  - Canal : transmission de **tous les incidents majeurs** (liés aux TIC et liés au paiement) et **cyber-menaces importantes** à **l'ACPR** via le portail **ONEGATE**, qui se chargera de transmettre aux autorités pertinentes.
    - Décommissionnement à partir du 17 janvier 2025 du canal Sharebox de la Banque de France, aujourd'hui utilisé pour les incidents de sécurité liés au paiement
  - Template: prévu par l'ITS sur le reporting des incidents majeurs
  - Format: .JSON (à confirmer)
  - Reporting selon ces nouvelles modalités dès l'entrée en application de DORA le 17 janvier 2025

2. DÉCLARATION DES SERVICES INFORMATIQUES EXTERNALISÉS

- **Remise annuelle à l'autorité compétente qui transmettra aux AES** et obligation de fournir ponctuellement un RoI à jour sur demande.

  – L'échéance de la première remise collective est en cours de définition au niveau des autorités européennes. L'information sera communiquée une fois confirmée.

→ Un corpus d'aide à la préparation du RoI est mis à disposition par les autorités européennes

https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act/preparation-dora-application

ACPR
BANQUE DE FRANCE

2. DÉCLARATION DES SERVICES INFORMATIQUES EXTERNALISÉS

- **Niveau de remise pour le reporting annuel des RoI: réduire le nombre de remises pour les groupes**

Entités (liste de cas non exhaustive)	Niveau de remise
Entités financières **qui ne font pas partie d'un groupe financier**	Remise **à l'ACPR**, **sur base individuelle**.
Groupes avec une tête de groupe **EC SI***	Remise **à la BCE**, **au plus haut niveau de consolidation**, **sur base consolidée.** ***Sauf*** *entités financières qui ne sont pas incluses dans le périmètre de consolidation prudentielle et organismes d'assurance : remise distincte sur base individuelle à l'autorité compétente.*
Groupes avec une tête de groupe **EC LSI***	Remise **à l'ACPR, au plus haut niveau de consolidation**, **sur base consolidée** (yc les organismes d'assurance FR). ***Sauf*** *entités financières qui ne sont pas incluses dans le périmètre de consolidation prudentielle : remise distincte sur base individuelle à l'autorité compétente.*
Groupes avec une tête de groupe **organisme d'assurance***	Remise **à l'ACPR, au plus haut niveau de consolidation**, **sur base consolidée.** ***Sauf*** *entités financières hors supervision de l'ACPR: remise distincte sur base individuelle à l'autorité compétente.*
Entités financières établies en FR **appartenant à un groupe de pays-tiers**, sans entreprise-mère établie dans l'UE:	Remise **à l'ACPR, sur base individuelle**.

** Uniquement si cette tête de groupe en FR est également la tête de groupe dans l'UE. Si l'entité au plus haut niveau de consolidation du groupe est située dans un autre Etat membre, la remise consolidée sera effectuée par cette entité à l'autorité compétente.*

2. DÉCLARATION DES SERVICES INFORMATIQUES EXTERNALISÉS

- **Modalités de remise des registres d'information (RoI) :**
  - Pour les établissements de crédit considérés comme importants (*Significant Institutions*):
    - Canal : transmission des RoI à la BCE via CASPER
    - Template: prévu par l'ITS sur le registre d'information (a priori extrêmement proche de celui utilisé pour le *dry run*)
    - Format: Excel
    - La BCE procédera aux vérifications et à l'envoi à l'EBA
  - Pour toutes les entités financières relevant de la compétence de l'ACPR:
    - Canal: transmission des RoI à l'ACPR via le portail ONEGATE (et non plus Sharebox lors du *dry run*)
    - Template: prévu par l'ITS sur le registre d'information
    - Format: Plain CSV (format attendu par les AES). L'outil de conversion (Excel -> Plain CSV) mis à disposition par les AES lors du *dry run* ne sera plus disponible
    - L'ACPR procédera aux vérifications et à l'envoi aux AES
- Date de la première remise en cours de discussion au niveau des autorités européennes

2. DÉCLARATION DES SERVICES INFORMATIQUES EXTERNALISÉS

- **Exercice volontaire de collecte des RoI organisé par les AES (*dry-run*) afin d'aider les entités financières dans la préparation de leur registre** :
  - Calendrier:
    - Début septembre : réception des registres (RoI) par l'ACPR et transmission aux AES
    - Courant octobre 2024 : après un contrôle qualité des données par les AES, l'ACPR se chargera de renvoyer les fichiers aux entités financières (répertoires dédiés Sharebox)
    - Novembre 2024 : atelier des AES à destination de l'industrie présentant les leçons tirées de l'exercice concernant la qualité des données
    - Décembre 2024 : publication par les AES d'un rapport sur la qualité des données agrégées
  - 62 registres ont été transmis aux AES par l'ACPR
  - Une dizaine d'établissements n'ont pu remettre, certains du fait du format de remise

3. NOTICE DORA ASSURANCE – GESTION DES RISQUES TIC

- **Objectif de la notice** :

  - *Accompagner les entités dans l'application des exigences DORA relatives à la gestion des risques liés aux TIC :*
    - DORA attend notamment des entités qu'elles revoient régulièrement leur cadre de gestion des risques liés aux TIC ;
    - La notice est élaborée en fonction des politiques et procédures internes attendues par le règlement DORA et les éléments mentionnés dans la notice aideront les entités à établir le rapport de revue du cadre de gestion des risques liés aux TIC.
  - *Recueillir un panel large des références réglementaires DORA relatives à la gestion des risques liés aux TIC :*
    - Depuis le règlement (UE) 2022/2554 du Parlement Européen et du Conseil du 14 décembre 2022 ;
    - Mais aussi depuis les règlement délégués (UE) 2024/1773 et 2024/1774 complétant le règlement précédent par des normes techniques de réglementation.

NOTICE DORA ASSURANCE – GESTION DES RISQUES TIC

- **La notice contient cinq parties principales et une annexe :**

1. *Introduction.*
   - Précisant notamment l'objet de la notice, ainsi que son champ d'application.

2. *Informations à communiquer dans le cadre du RSR*
   - Des informations relatives au cadre de gestion des risques liés aux TIC seront demandées dans le RSR.

3. *Outils, méthodes, processus et politiques de gestion du risque lié aux TIC*
   - Précisions sur les documents que les entités du secteur de l'assurance devront élaborer et mettre en œuvre dans le cadre de la gestion des risques liés aux TIC.
   - Liens vers les références réglementaires de gestion du risque TIC du règlement DORA et des normes techniques de réglementation le complétant.

4. *Cadre simplifié de gestion du risque lié aux TIC*
   - Application du principe de proportionnalité pour les petits ORPS.

5. *Rapport sur le réexamen du cadre de gestion du risque lié aux TIC*
   - Le cadre de gestion du risque lié aux TIC doit être documenté et réexaminé au moins une fois par an, ou périodiquement selon la taille de l'entité.
   - Ce réexamen doit faire l'objet d'un rapport qui est remis, sur demande, à l'ACPR.

Annexe
   - Détaillant la structure et le contenu du rapport sur le réexamen du cadre de gestion du risque lié aux TIC.

NOTICE DORA ASSURANCE – GESTION DES RISQUES TIC

- **À qui s'adressent les différentes parties de la notice ?**

Parties de la notice :	Informations à communiquer dans le cadre du RSR	Outils, méthodes, processus et politiques de gestion du risque lié aux TIC	Cadre simplifié de gestion du risque lié aux TIC	Rapport sur le réexamen du cadre de gestion du risque lié aux TIC
Aux **organismes** d'assurance ou de réassurance **relevant du régime « Solvabilité II »**	Oui	Oui	Non	Oui
Aux **petits ORPS*** qui comptent entre quinze et cent affiliés au total	Oui	Non	Oui	Oui**
Aux **ORPS*** qui comptent au moins cent affiliés au total	Oui	Oui	Non	Oui
Aux **intermédiaires** d'assurance, intermédiaires de réassurance et intermédiaires d'assurance à titre accessoire, qui ne sont **ni des microentreprises, ni des petites ou moyennes entreprises**	Non	Oui	Non	Oui

*ORPS : organisme de retraite professionnelle supplémentaire
Pour les petits ORPS, il s'agit du rapport sur le réexamen du cadre **simplifié de gestion du risque lié aux TIC

NOTICE DORA ASSURANCE – GESTION DES RISQUES TIC

- **Focus sur le rapport sur le réexamen du cadre de gestion du risque lié aux TIC**

  - *Le cadre de gestion du risque lié aux TIC doit être documenté et réexaminé au moins une fois par an, ou périodiquement selon la taille de l'entité*
    - Il l'est également en cas de survenance d'incidents majeurs liés aux TIC.

  - *Le réexamen s'inscrit dans un processus d'amélioration permanente sur la base des enseignements tirés de la mise en œuvre et du suivi*
    - Il tient compte des conclusions tirées des tests de résilience opérationnelle numérique ou des processus d'audit pertinents.

  - *Le réexamen est matérialisé par un rapport « sur le réexamen du cadre de gestion du risque lié aux TIC » qui est présenté à l'ACPR à sa demande, dans un format électronique interrogeable*

  - *Ce rapport contient notamment :*
    - Les principales insuffisances relevées, risques et anomalies détectées ;
    - Les mesures correctives engagées pour remédier aux insuffisances relevées, date de réalisation prévisionnelle de ces mesures et état d'avancement de leur mise en œuvre à la date de rédaction du présent rapport ;
    - Les modalités de suivi des recommandations résultant des contrôles permanents (outils, personnes en charge);
    - Les modalités de vérification de l'exécution dans des délais raisonnables des mesures correctrices décidées au sein de l'entreprise par les personnes compétentes.

  - *Le rapport établi au titre de la première année d'entrée en vigueur du cadre réglementaire DORA (2025) décrit les éléments du cadre de gestion des risques liés aux TIC et souligne les sujets encore en développement ou qui restent à approfondir.*

NOTICE DORA ASSURANCE – PROCHAINES ÉTAPES

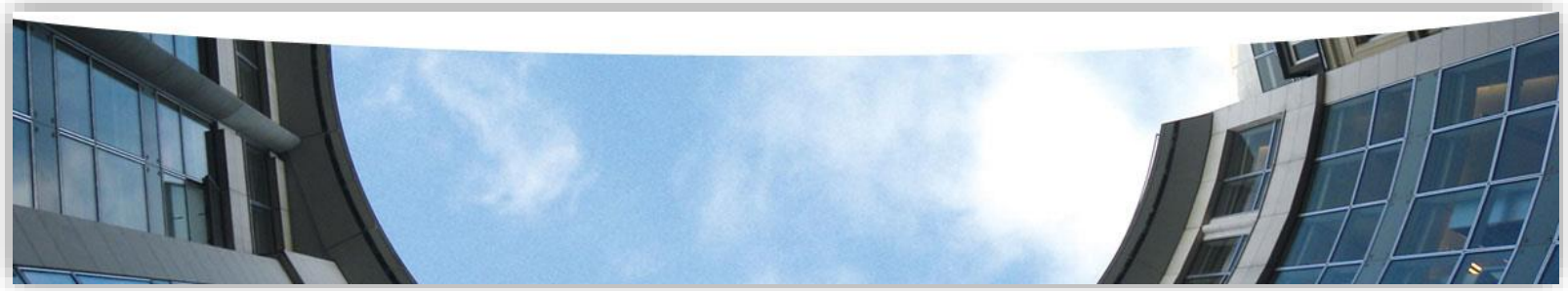
1
- Partage de la notice avec les entités pour une consultation ouverte jusqu'au mois de novembre

2
- Présentation de la notice à la CCAP de novembre puis au Collège de l'ACPR de décembre 2024

3
- Entrée en vigueur de DORA le 17 janvier 2025

4
- Tous les organismes devront établir au plus tard leur 1er rapport sur la revue du cadre de gestion des risques liés aux TIC en 2026 (sur la base de l'exercice 2025).
- Mais les organismes sont encouragés à s'y préparer dès 2025, notamment pour les plus importants, auxquels il est recommandé de rédiger un rapport « à blanc » pour juin 2025.

AVEZ-VOUS DES QUESTIONS ?



- Pour toute question relative au règlement DORA, nous invitons les fédérations professionnelles à collecter et à nous remonter les questions de leurs adhérents.

- Les services de l'ACPR peuvent aussi être contactés à l'adresse suivante si besoin: 2760-DORA-UT@acpr.banque-france.fr

ANNEXES

CADRE DE GESTION DES RISQUES LIÉS AUX TIC

IMPLICATION DE LA GOUVERNANCE DANS LA RESILIENCE OPERATIONNELLE NUMERIQUE

- Articulation entre stratégie globale et stratégie de résilience opérationnelle numérique : définition du cadre et tolérance à l'incidence liée aux perturbations

- Un rôle actif de l'organe de direction, responsable de la gestion des risques liés aux TIC
  - « Responsabilité entière et ultime »
  - « Engagement continu »
  - Ayant des connaissances et des compétences suffisantes

- Allocation claire des rôles et responsabilités
  - Une fonction de contrôle indépendante qui a la responsabilité de la gestion et de la surveillance du risque lié aux TIC
  - Mettre en place des fonctions de gestion dédiées à la surveillance des accords avec les prestataires tiers de services TIC ou à la gestion des crises
  - Un canal de notification interne doit être mis en place pour informer l'organe de direction des accords conclus avec les prestataires
  - Organisation selon le modèle reposant sur trois lignes de défense, ou pour établir un modèle de gestion des risques et de contrôle internes

- Un cadre de gestion des risques revu et documenté au sein d'un rapport
  - Audit interne régulier
  - Évaluation approfondie après des changements majeurs (architecture réseau, SI)

ACPR
BANQUE DE FRANCE

LISTE DES ATTENDUS DE DORA

Nom de l'attendu (document, livrable, stratégie, politique interne)	Référence	Dispenses éventuelles
Cadre de gouvernance et de contrôle interne du risque ICT	Article 5.1	Les entités soumises au cadre simplifié de l'article 16.
Stratégies garantissant des normes élevées de disponibilité, authenticité, intégrité et confidentialité des données	Article 5.2.b	
Plan d'audit des TIC	Article 5.2.f	
Politique concernant les services TIC fournis par des prestataires tiers	Article 5.2.h	
Cadre de gestion du risque TIC (inclut : stratégie de résilience opérationnelle)	Articles 6.1 et 6.8	
Rapport sur le réexamen du cadre de gestion du risque TIC (sur demande de l'autorité compétente)	Article 6.5	
Stratégie globale multifournisseurs (facultatif)	Article 6.9	
Inventaires des risques ICT sur les fonctions métiers	Article 8.6	
Politique de la sécurité de l'information	Article 9.4.a	
Politiques qui limitent l'accès physique ou logique aux actifs ICT	Article 9.4.c	
Politiques et protocoles d'authentification forte	Article 9.4.d	
Politiques sur la gestion du changement ICT	Article 9.4.e	
Stratégies en matière de mises à jour et correctifs	Article 9.4.f	
Politique de continuité des activités de TIC	Article 11.1	
Plan de réponse et de rétablissement des TIC	Article 11.3	
Registre des activités lors de l'activation de PCA / plan de réponse	Article 11.8	
Estimation du coût annuel des incidents majeurs	Article 11.10	
Politiques et procédures de sauvegarde	Article 12.1.a	
Procédures et méthodes de restauration et rétablissement	Article 12.1.b	
Examens post-incident	Article 13.2	
Programmes de sensibilisation et formation du personnel	Article 13.6	
Plan de communication	Article 14.1	
Processus de gestion des incidents	Article 17.1	
Rapport d'incident initial	Article 19.4.a	
Rapport d'incident intermédiaire	Article 19.4.b	
Rapport d'incident final	Article 19.4.c	
Programme de tests de résilience	Article 24.1	Les microentreprises sont dispensées.
Procédures et stratégies pour traiter les problèmes identifiés par les tests	Article 24.5	Les microentreprises sont dispensées.
Plans de mesures correctives	Article 26.5	Les microentreprises sont dispensées.
Stratégie en matière de risques liés aux prestataires TIC tiers (inclut une politique sur l'externalisation des fonctions critiques et importantes)	Article 28.2	
Registre d'information sur tous les contrats d'externalisation TIC	Article 28.3	
Information sur tous les projets d'accord contractuel portant sur une externalisation TIC	Article 28.3	
Stratégies de sortie	Article 28.8	
Plans de transition	Article 28.8	
Mesures d'urgence lors de l'activation de la stratégie de sortie	Article 28.8	

ACPR
BANQUE DE FRANCE