FRANCE INVEST

DORA - Digital Operational Resilience Act

10 octobre 2023

Règlement sur la résilience opérationnelle numérique du secteur financier

Contexte

- Le secteur financier est vulnérable à des cyberattaques mais les risques cyber sont partiellement traités au niveau européen :
  - Des règles **générales** s'appliquant partiellement au secteur + une mise en œuvre inégale ;
  - Des règles **pour les services financiers** morcelées, incohérentes et fragmentées.
- Proposition de règlement **DORA** publiée par la Commission européenne le 24 septembre 2020, dans le cadre d'un train de mesures contenant :
  - une stratégie en matière de finance numérique,
  - une proposition sur les marchés de crypto-actifs (MiCA),
  - une proposition sur la technologie des registres distribués (DLT).
- **DORA se substitue à la Directive NIS2** (Network and Information Security, 2022) **pour le secteur financier** et complète la Directive CER (sur la résilience des entités critiques, 2022), le Règlement SCA (Cybersecurity Act, 2019) et le Règlement CRA (Cyber Resilience Act, en cours de négociation)

- **Entrée en application le 17 janvier 2025.**

https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022R2554

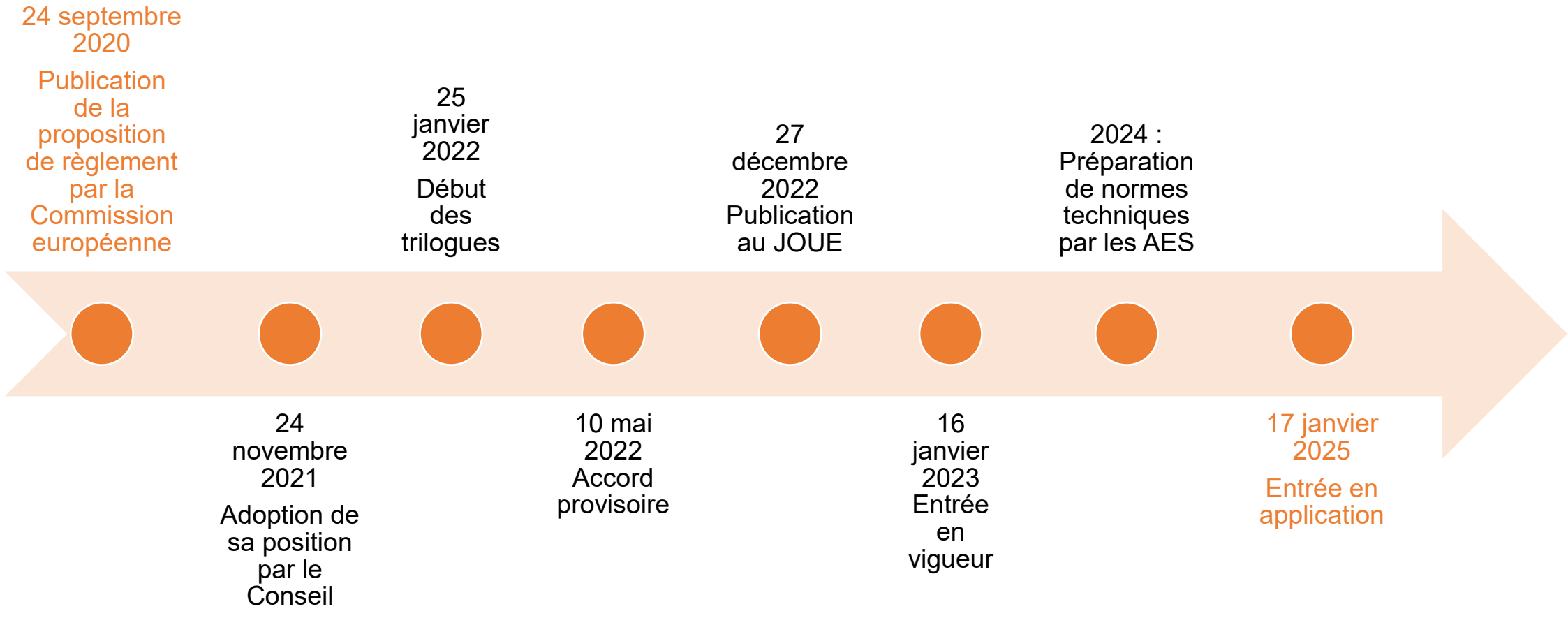
Points clés

Des exigences uniformes pour la sécurité des réseaux et des systèmes d'information des entreprises et des organisations actives **dans le secteur financier** ainsi que des **tiers critiques** qui leur fournissent des services liés aux technologies de l'information et de la communication (TIC).

- Presque toutes les entités financières seront soumises à la nouvelle réglementation
  - **Notamment les gestionnaires de FIA au-dessus des seuils de la directive AIFM (100 millions EUR et 500 millions EUR)**
- Obligations applicables aux entités financières :
- Obligations liées aux contrats avec les prestataires tiers de services TIC
- Cadre de supervision des prestataires de services TIC critiques
- Règles relatives à la coopération entre autorités

NB : Application du principe de proportionnalité : « Les entités financières mettent en œuvre les règles énoncées au chapitre II conformément au principe de proportionnalité, en tenant compte de leur taille et de leur profil de risque global ainsi que de la nature, de l'ampleur et de la complexité de leurs services, activités et opérations ».

Calendrier


24 septembre 2020
Publication de la proposition de règlement par la Commission européenne
24 novembre 2021
Adoption de sa position par le Conseil
25 janvier 2022
Début des trilogues
10 mai 2022
Accord provisoire
27 décembre 2022
Publication au JOUE
16 janvier 2023
Entrée en vigueur
2024 : Préparation de normes techniques par les AES
17 janvier 2025
Entrée en application

Définitions

- *«résilience opérationnelle numérique» : la capacité d'une entité financière à développer, garantir et réévaluer son intégrité et sa fiabilité opérationnelles en assurant directement ou indirectement par le recours aux services fournis par des prestataires tiers de services TIC, l'intégralité des capacités liées aux TIC nécessaires pour garantir la sécurité des réseaux et des systèmes d'information qu'elle utilise, et qui sous-tendent la fourniture continue de services financiers et leur qualité, y compris en cas de perturbations*

- *«risque lié aux TIC»: toute circonstance raisonnablement identifiable liée à l'utilisation des réseaux et des systèmes d'information qui, si elle se concrétise, peut compromettre la sécurité des réseaux et des systèmes d'information, de tout outil ou processus dépendant de la technologie, du fonctionnement et des processus ou de la fourniture de services en produisant des effets préjudiciables dans l'environnement numérique ou physique;*

Principales obligations pour les entités financières

- Gestion du risque lié aux TIC
- Reporting sur les incidents et cybermenaces
- Tests de résilience opérationnelle numérique
- Gestion des risques liés aux tiers
- Partage d’informations concernant les menaces et vulnérabilités cyber

Gestion du risque lié aux TIC

- Disposer d'un **cadre de gouvernance** interne et de contrôle placé sous la responsabilité de l'organe de **direction**.
- Avoir un cadre de **gestion des risques** actualisé et audité.
- Utiliser des systèmes, protocoles et outils de TIC appropriés, fiables et résilients.
- **Identifier** toutes les fonctions, toutes les sources de risqué et les actifs informationnels, les processus qui dépendent de prestataires de services liés aux TIC.
- **Surveiller** le fonctionnement de leurs systèmes et outils TIC de manière continue et en assurer la résilience, la continuité et la disponibilité.
- **Détecter** les activités anormales et identifier les points de défaillance.
- Mettre en place et tester régulièrement une **politique de continuité des activités de TIC et un plan de réponse et de rétablissement** des TIC. Avoir une fonction de **gestion de crise**. Fournir aux autorités compétentes, sur leur demande, une estimation des coûts et pertes causés par les incidents majeurs.
- Mettre en place des **politiques de sauvegarde et des méthodes de restauration et de rétablissement**.
- Avoir des capacités pour **rassembler l'information** sur leurs vulnérabilités et cybermenace, analyser leur impact potentiel, mettre en place des examens post incidents, intégrer les enseignements, contrôler l'efficacité de la stratégie.
- Mettre en place des **plans de communication** sur les incidents en interne, aux clients et aux contreparties ainsi qu'au public, le cas échéant.

Reporting sur les incidents et cybermenaces

- Exigences générales :
  - Établir et mettre en œuvre un **processus de gestion** pour suivre et **enregistrer** les incidents liés aux TIC
  - **Catégoriser** les incidents liés aux TIC et cybermenaces (sur la base de critères définis par DORA et à développer par les AES)

- Reporting aux **autorités compétentes** :
  - Des incidents **majeurs**
  - Notification **volontaire** des cyber menaces importantes aux autorités compétentes, lorsque les entités financières estiment que la menace est pertinente pour le système financier, les utilisateurs de services ou les clients.

- Information des **clients** :
  - Lorsqu'un **incident majeur** lié aux TIC survient et a une incidence sur les intérêts financiers des clients, les entités financières informent leurs clients de cet incident majeur lié aux TIC et des mesures qui ont été prises pour atténuer les effets préjudiciables de cet incident sans retard injustifié.
  - En cas **de cybermenace importante**, les entités financières informent, le cas échéant, leurs clients susceptibles d'être affectés de toute mesure de protection appropriée que ces derniers pourraient envisager de prendre.

Tests de résilience opérationnelle numérique

- Tests de base (pour toutes les entités du secteur financier) :
  - Mettre en place un programme de test, réalisé par une entité indépendante (interne ou externe), classer et remédier aux problèmes identifiés et tester tous les systèmes critiques au moins une fois par an.

- Des tests avancés d'outils, de systèmes et de processus de TIC sur la base de **tests de pénétration** fondés sur la menace :
  - Pour les entités financières identifiées par les autorités compétentes
  - Sur plusieurs, voire la totalité, des fonctions critiques ou importantes
  - Au moins tous les 3 ans (cette fréquence peut être adaptée par l'autorité compétente selon les cas)
  - Utilisation de testeurs internes et externes

Gestion des risques liés aux tiers

- Principes généraux :
  - Pleine responsabilité de l'entité financière + principe de proportionnalité
  - Adopter et revoir régulièrement leur stratégie sur les risques liés aux prestataires tiers de services TIC
  - Tenir et actualiser un registre des arrangements contractuels avec des prestataires de services TIC :
    - distinguer ceux qui couvrent des fonctions critiques
    - communiquer au moins une fois par an aux autorités compétentes
    - informer en temps utile l'autorité compétente de tout projet d'accord contractuel portant sur l'utilisation de services TIC qui soutiennent des fonctions critiques ou importantes + lorsqu'une fonction est devenue critique ou importante.
  - Procéder à des vérifications **préalables** à la conclusion d'un contrat avec un prestataire de services TIC :
    - pour les services TIC qui soutiennent des fonctions critiques ou importantes, mettre en place des stratégies de sortie
- **Cadre de supervision pour les prestataires critiques :**
  - Désignation par les AES
  - Les AES auront le pouvoir de les surveiller et émettront des recommandations
  - Mise en place d'un forum de supervision

Partage d’informations

- Les entités financières peuvent échanger entre elles des informations et des renseignements sur les cybermenaces :
  - notamment des indicateurs de compromis, des tactiques, des techniques et des procédures, des alertes de cybersécurité et des outils de configuration

Des règles complémentaires à venir

- Sur la gestion du risque lié aux TIC :
  - Outils, méthodes, processus et politiques de gestion du risque lié aux TIC
  - Cadre simplifié de gestion des risques liés aux TIC
  - Tests de pénétration fondés sur la menace

- Reporting des incidents liés aux TIC
  - Critères de classification des incidents liés aux TIC
  - Notification des incidents majeurs liés aux TIC
  - Formulaires, les modèles et les procédures types pour notification des incidents
- Structure de supervision
  - Coopération entre les ESAs et autorités nationales sur la structure de supervision
  - Supervision des prestataires tiers de services TIC

=> 2 paquets de consultations:

- Mi-juin à mi-septembre 2023
- Novembre 2023 à février 2024

Annexe

Gestion du risque lié aux TIC
Gouvernance et organisation

- Obligation de mettre en place une **gouvernance** et un **contrôle interne** pour la gestion du risque lié aux TIC
- L'**organe de direction** doit définir, approuver, superviser et est responsable pour la mise ne œuvre du cadre de la gestion du risque liés aux TIC :
  - Responsable ultime de la gestion des risques TIC
  - Stratégies assurant la disponibilité, authenticité, intégrité et confidentialité des données
  - Définir des rôles et responsabilités pour les fonctions liées aux TIC
  - Définir et approuver la stratégie de résilience opérationnelle digitale incl. le niveau approprié de tolérance au risque lié aux TIC
  - Définir et approuver une politique de continuité des activités et de plans de réponse et de rétablissement
  - Approuver et revoir les plans d'audit TIC
  - Alloue et revoit un budget approprié incluant la sensibilisation et la formation pour tout le personnel
  - Approuve et revoit les politiques concernant le recours aux prestataires de services TIC
  - Doit être informé des incidents TIC majeurs, de leur impact et des mesures apportées
- Obligation d'établir un poste pour gérer les accords conclus avec les prestataires de services TIC ou de désigner un membre du senior management responsable de superviser l'exposition au risque TIC.
- Les membres de l'organe de direction doivent avoir des connaissances et compétences actualisées pour comprendre et évaluer les risques TIC et leur impact (formation régulière).