Digital Operational Resilience Act – DORA

Résilience opérationnelle numérique

Séminaire AEFR du 17 mai 2023

mazars

01

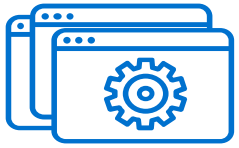
Pourquoi DORA ?

Résilience opérationnelle

Pourquoi DORA ?

- La directive européenne Digital Operational Resilience Act-DORA établit des exigences uniformes relatives au risque cyber des entités financières de l'Union Européenne.
- DORA répond aux 3 principaux enjeux suivants :

Transformation numérique et interconnexion

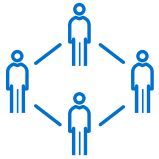


Carences identifiées dans la résilience opérationnelle numérique

Disparités législatives au sein de l'UE

Renforcer la résilience opérationnelle numérique pour l'ensemble du secteur financier.

Résilience opérationnelle
Champs d’application



Une réglementation qui touche l’ensemble du secteur financier.

Banques et sociétés financières

- Etablissements de crédit
- Etablissements de paiement
- Etablissements de monnaie électronique
- Entreprises d’investissement

Assurances

- Entreprises d’assurance et de réassurance
- Intermédiaires d’assurance, de réassurance et d’assurance à titre accessoire
- Institutions de retraite professionnelle

Gestion d’actifs

- Sociétés de gestion
- Dépositaires centraux de titres
- Contreparties centrales
- Plateformes de négociation
- Référentiels centraux
- Gestionnaires de fonds d’investissement alternatifs
- Référentiels des titrisations

Observateurs

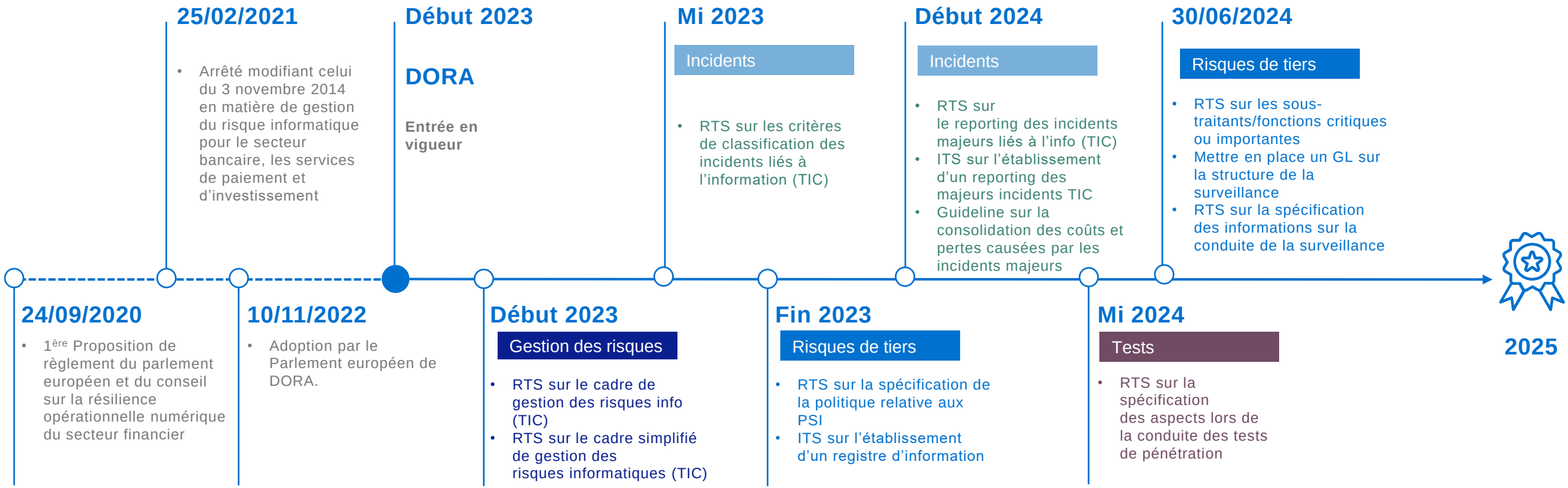
- Agences de notation de crédit
- Contrôleurs légaux des comptes et cabinets d’audit
- Administrateurs d’indices de référence d’importance critique

Prestataires

- Tiers prestataires de services informatiques
- Prestataires de services sur cryptoactifs
- Emetteurs de cryptoactifs et de jetons
- Prestataires de services de communication de données
- Prestataires de services de financement participatif

- L’application des règles en matière de résilience opérationnelle numérique est appliquée de façon proportionnée aux entreprises concernées en fonction de la taille, des profils d’activité ou de l’exposition au risque numérique.

Résilience opérationnelle
Dans quels délais ?



- *RTS : Regulatory and Technical Standards*
- *ITS : Implementing Technical Standards*

02

Les 5 piliers de DORA

Résilience opérationnelle
Les cinq piliers du règlement DORA

Cadre de gestion des risques informatiques

- Gouvernance et organisation appropriée
- Cadre de gestion des risques informatiques adapté et resilient
- Mesures techniques de résilience harmonisées

Gestion des incidents liés à l'informatique

- Processus de gestion des incidents liés à l'informatique formalisé et effectif
- Classification des incidents
- Notification aux autorités des incidents informatiques majeurs

Partage d'informations

- Dispositif d'échange d'informations entre les entreprises financières sur les cybermenaces et dysfonctionnements

Tests de résilience opérationnelle numérique

- Programme de tests de résilience sur les outils et SI
- Tests de résilience avancés (tests de pénétration par la menace)
- Diligences approfondies sur les compétences, l'expertise et l'intégrité des testeurs

Gestion du risque de tiers prestataires de services informatiques

- Suivi rigoureux du risque lié aux prestataires de services informatiques
- Supervision des prestataires informatiques critiques par les AES

Résilience opérationnelle
Cadre de gestion des risques informatiques

- DORA conforte les règles de gouvernance et de gestion des risques en vigueur.

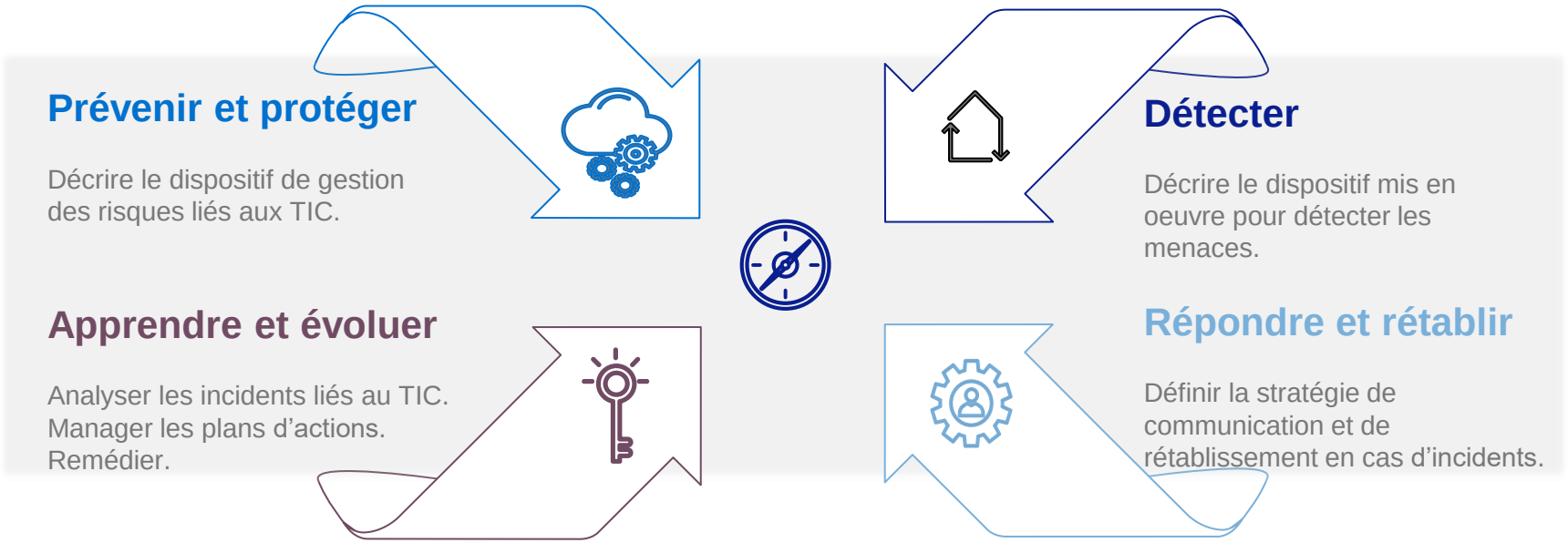
- Les entités financières doivent :
  - mettre en œuvre un cadre formel de gouvernance et de gestion des risques liés aux TIC,
  - mettre en place et maintenir des systèmes et outils de TIC résilients.

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

- Gouvernance renforcée :
  - Niveau approprié de tolérance aux risques liés aux TIC
  - Politique de continuité des activités liées aux TIC
  - Plan de reprise d'activité
  - Investissement en matière de TIC
  - Formation des membres de l'organe de direction
  - Stratégie de résilience opérationnelle numérique formalisée

IDENTIFIER

Définir des objectifs clairs en matière de sécurité de l'information.

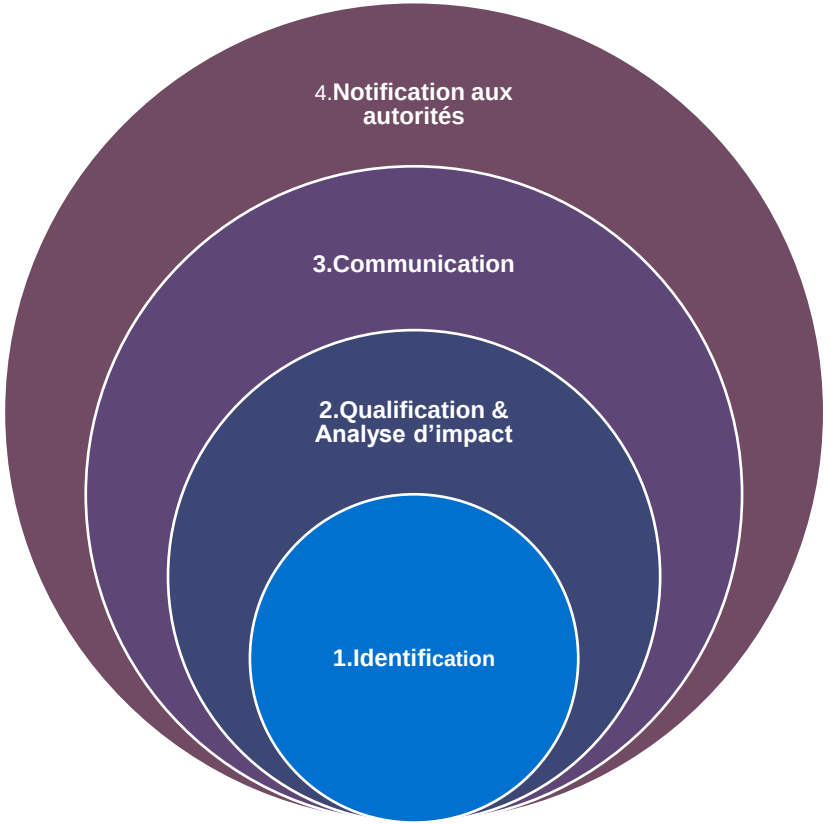


COMMUNIQUER

Définir et décrire la stratégie de communication.

Résilience opérationnelle
Notification des incidents

- DORA harmonise la gestion des incidents informatiques, notamment les plus impactant en définissant un cadre structuré en 4 grandes étapes:



- Les étapes 1 & 2 sont généralement en place, répondant aux bonnes pratiques ITIL ou Cobit. DORA énonce de grands axes d'analyse pour la qualification :
  a) *le nombre d'utilisateurs ou de contreparties financières touchés*
  b) *la durée de l'incident, y compris les interruptions de service*
  c) *la répartition géographique et les zones touchées, en particulier si celui-ci touche plus de deux États membres*
  d) *les pertes de données occasionnées telles que la perte d'intégrité, la perte de confidentialité ou la perte de disponibilité*
  e) *la gravité des effets de l'incident et la criticité des services touchés*
  f) *les conséquences économiques, en termes absolus et relatifs*

- La communication attendue lors d'un incident informatique est davantage orientée vers les utilisateurs internes, les partenaires au sens (très) large :
  - *Les plans pour la communication à l'intention du personnel, des parties prenantes externes et des médias, conformément à l'article 13, et pour la notification aux clients, les procédures internes de remontée des incidents, y compris les plaintes des clients liées aux TIC, ainsi que pour la fourniture d'informations aux entités financières qui agissent en tant que contreparties, le cas échéant;*

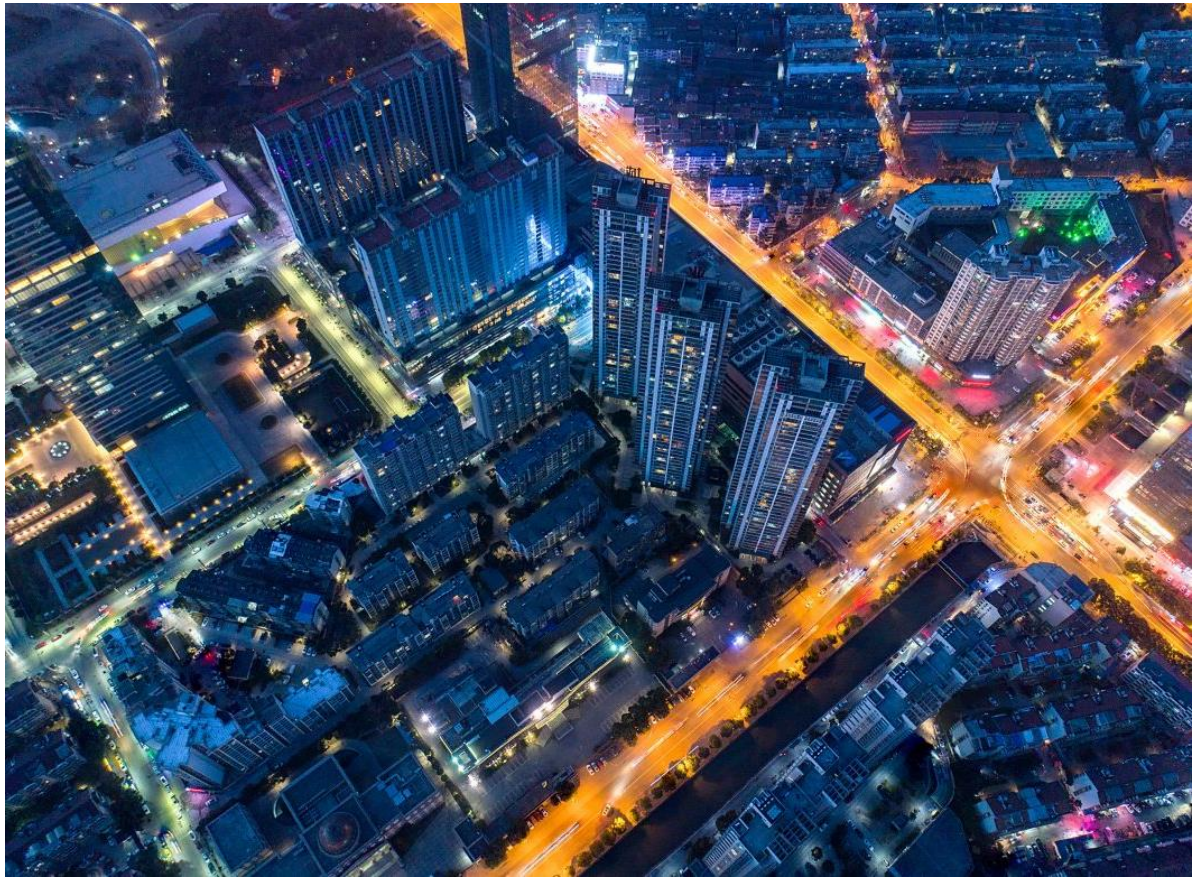
- La notification vers les autorités concerne uniquement les incidents majeurs dont une nomenclature harmonisée sera publiée dans les RTS. Un dossier dédié sera à formaliser selon un calendrier strict (jour j, une semaine puis un mois).

Résilience opérationnelle
Partage d’information

Notion portée par l’article 40, sur la possibilité de partager autour des dispositifs de défense et des menaces entre les entités financières. Il s’agit davantage d’un point de vigilance sur les règles de partage.

Améliorer la résilience opérationnelle numérique des entités financières, le partage se déroule au sein de communautés d’entités financières de confiance;

Par la nature potentiellement sensible des informations partagées, les échanges sont régis par des règles de conduite dans le plein respect de la confidentialité des affaires, de la protection des données à caractère personnel et des lignes directrices sur la politique de concurrence.



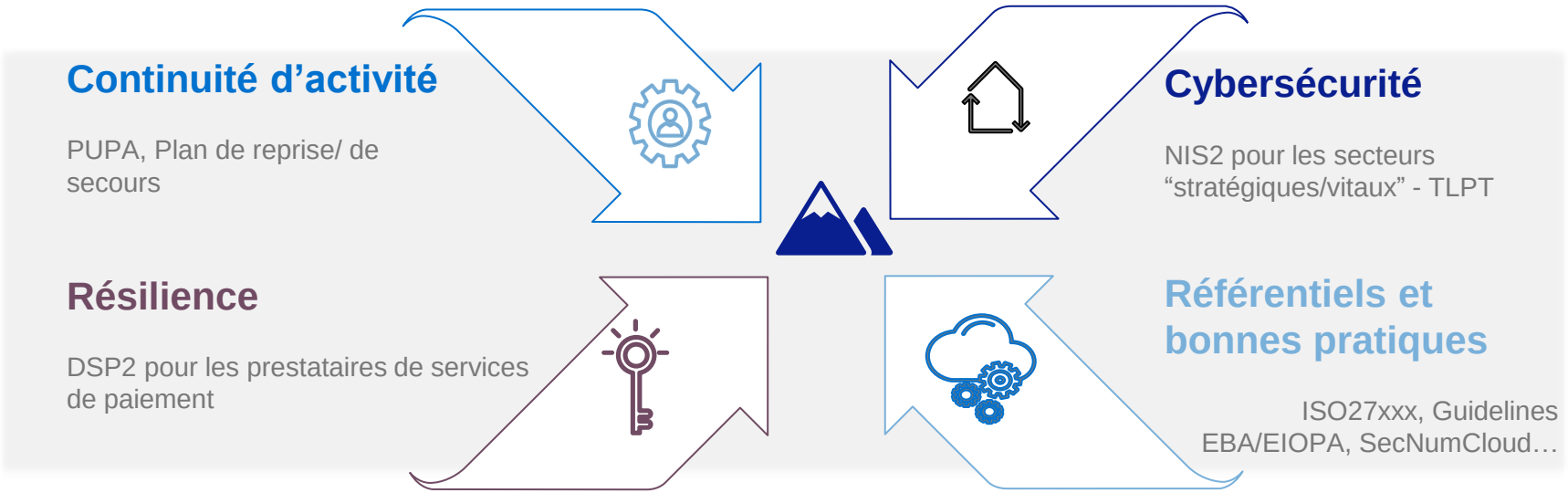
Résilience opérationnelle
Tests de résilience

- DORA rassemble les grands principes de résilience énoncés dans les derniers textes européens ou sectoriels, et se place ainsi comme un texte « ombrelle ». Il ne s'agit pas d'une surcouche, plutôt d'une consolidation des dispositifs répondant des exigences éparses.

- DORA propose une vision holistique des risques (ou menaces) pouvant affecter la résilience qu'ils soient informatiques, cyber ou physiques. Ce qui nécessite la définition d'une stratégie globale de résolution donc de tests selon les différents scénarios de menace définis par l'entité.

EVALUER

Identifier et mesurer les risques et menaces



TESTER

Définir et décrire la stratégie de tests

Résilience opérationnelle
Gestion du risque de tiers

- DORA conforte les principes de gestion des tiers des lignes directrices de l'EBA :

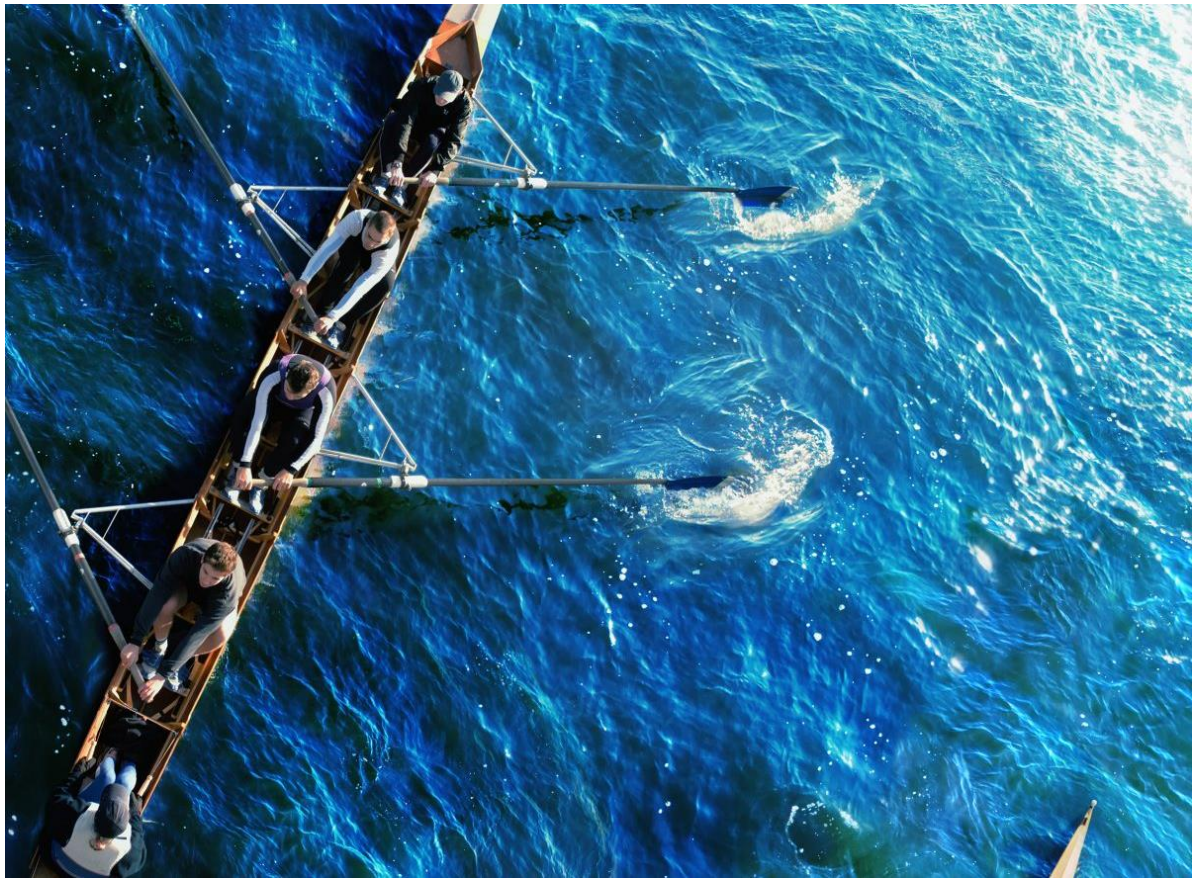
Maintien de la responsabilité du risque	Proportionnalité dans la gestion du risque	Mise en œuvre d'une véritable stratégie
Registre	Étude précontractuelle des risques	Stratégie de sortie

- Cadre de surveillance des prestataires critiques

Possibilité de demander son identification comme prestataire critique

Liste publiée par les AES* sur la base de critères

- Tous les prestataires (y compris intra-groupe).
- Publication annuelle par les AES de la liste des prestataires critiques au niveau de l'UE.



Résilience opérationnelle
Gestion du risque de tiers

Extrait de l’article 27 – clauses contractuelles (2)

- *Les accords contractuels relatifs à l’utilisation de services informatiques comportent au moins les éléments suivants:*

(a) une description claire et exhaustive de tous les services et fonctions qui seront fournis par le tiers prestataire de services informatiques,

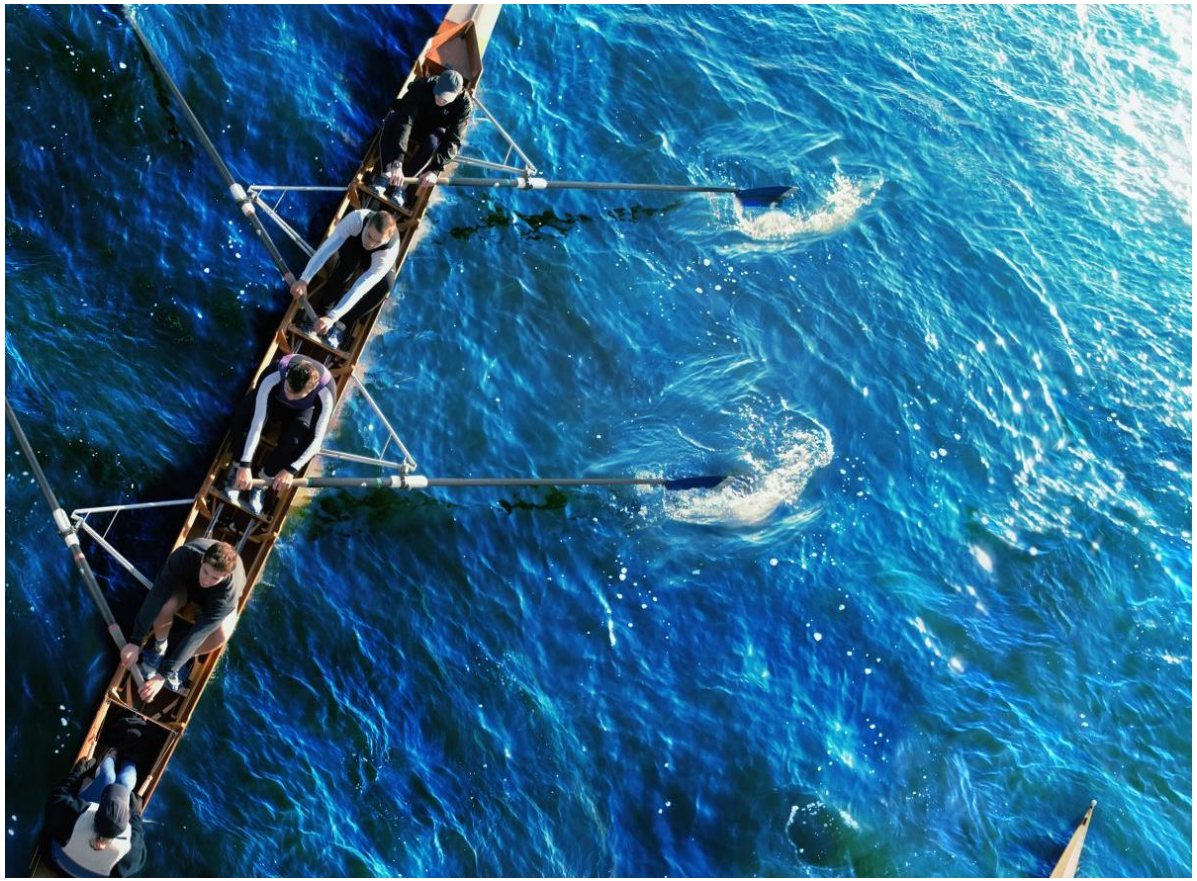
(b) les lieux où les services et fonctions visés par le contrat ou la sous-traitance seront fournis et où les données seront traitées,

(c) des dispositions sur l’accessibilité, la disponibilité, l’intégrité, la sécurité et la protection des données à caractère personnel et sur la garantie de l’accès, de la récupération et de la restitution,

(d) des descriptions complètes des niveaux de service, y compris leurs mises à jour et révisions, et des objectifs de performance quantitatifs et qualitatifs

(e) les délais de préavis et les obligations de notification du tiers prestataire de services informatiques à l’entité financière, y compris la notification de tout développement susceptible d’avoir une incidence significative

(f) l’obligation pour le tiers prestataire de services informatiques de fournir, sans frais supplémentaires ou à un coût déterminé ex ante, une assistance en cas d’incident lié à l'informatique;



Résilience opérationnelle
Gestion du risque de tiers

Extrait de l'article 27 – clauses contractuelles (2/2)

- *Les accords contractuels relatifs à l'utilisation de services informatiques comportent au moins les éléments suivants:*

(f) l'obligation pour le tiers prestataire de services informatiques de fournir, sans frais supplémentaires ou à un coût déterminé ex ante, une assistance en cas d'incident lié à l'informatique;

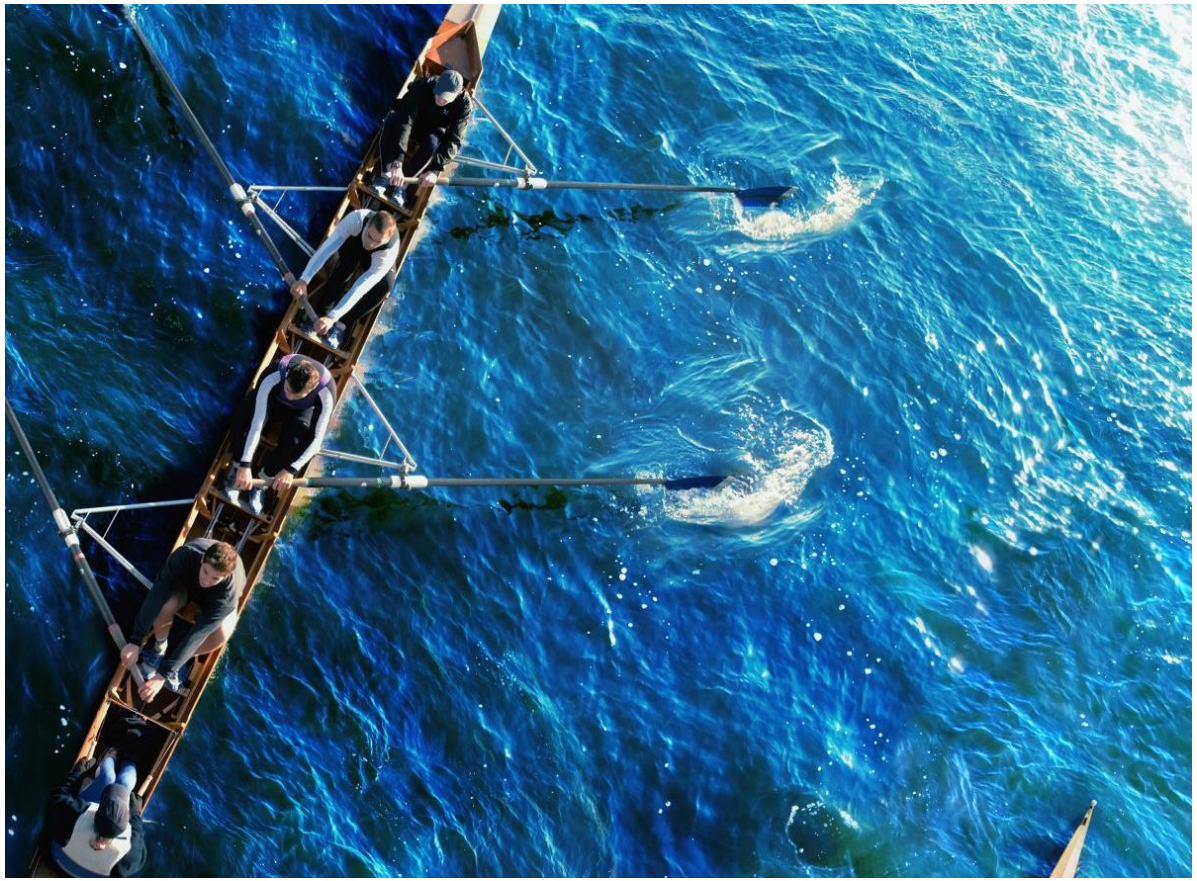
(g) l'obligation pour le tiers prestataire de services informatiques de mettre en œuvre et de tester des plans d'urgence et de mettre en place des mesures, des outils et des politiques de sécurité en matière de TIC;

(h) le droit d'assurer un suivi permanent des performances du tiers prestataire de services informatiques, qui comprend i) les droits d'accès, d'inspection et d'audit par l'entité financière , ii) le droit de convenir d'autres niveaux d'assurance si les droits d'autres clients sont affectés; iii) l'engagement de coopérer pleinement lors des inspections sur place effectuées;

(i) l'obligation pour le tiers prestataire de services informatiques de coopérer pleinement avec les autorités compétentes

(j) les droits de résiliation et le délai de préavis minimal correspondant pour la résiliation du contrat;

(k) les stratégies de sortie, en particulier la fixation d'une période de transition adéquate obligatoire.



03

Facteurs clés de succès

7 facteurs clés de succès

1.Mode projet

Démarrer au plus tôt en mode projet en embarquant les bons acteurs

2.Stratégie

Définir une stratégie globale de résilience

3.Culture du risque

Développer la culture autour des risques TIC

4.Gestion des tiers

Faire évoluer sa relation avec ses partenaires TIC

5.Capitalisation

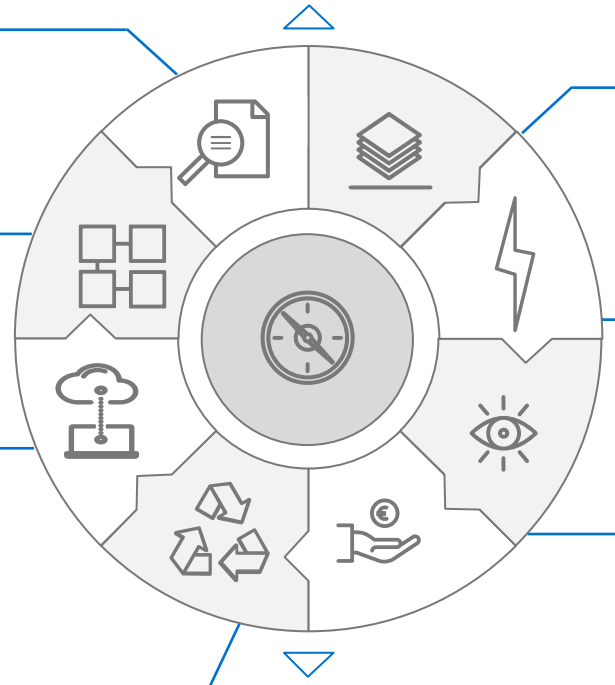
Consolider les dispositifs relatifs à la résilience et gestion des risques IT (yc Cyber)

6.Veille

Disposer d'une vision holistique des règlementations en cours et à venir

7.Instances dirigeantes

Sensibiliser le top management aux enjeux de la réglementation



Facteurs clés de succès

Passer de la gestion du risque opérationnel à la résilience opérationnelle

Risk Appetite Framework et Statement IT

CADRAGE

- Valider le périmètre de l'étude DORA
- Identifier les acteurs clés
- Organiser les ateliers

GAP ANALYSIS

- Prendre connaissance de l'existant
- Identifier les impacts de DORA sur les 5 piliers

PLAN D'ACTIONS & FEUILLE DE ROUTE

- Evaluer les impacts identifiés
- Proposer des recommandations
- Définir un plan d'action pragmatique

Diffusion de la culture du risque au sein de l'entité