BIA GROUPE

Digital **O**perationnal **R**esiliency **A**ct

Enjeux pour la Finance et les ESN

Sommaire

1. **DORA et la gestion des risques informatiques**
    - ISO27000 / Bâle 3 / OIV / SRI / DSP2 / RGPD / DSP2
    - DORA
2. **Impact pour les prestataires de services**
    - Impact pour les ESN
    - DORA s’inspire de ISO 27000

DORA
et la gestion des risques informatiques

ISO27000 / Bâle 3 / OIV / SRI / DSP2 / RGPD / DSP2

De nombreuses initiatives ont été prises pour renforcer la résilience du système financier à la suite de la crise financière de 2007 et aux nombreuses cyber-attaques afin de palier aux manquements et se prémunir du risque de réputation. Elles se traduisent par des normes, des directives Européennes, des lois d'orientation ou bien sont incluses dans des cadres réglementaires plus généraux.

- **ISO 27000** est une série de normes conçues en 2009 pour protéger les actifs d'information des organisations en les guidant dans leur gestion des risques liés au systèmes d'information, de la formulation à l'exécution, de la supervision, de l'ajustement, de l'évaluation et de la maintenance, afin de s'assurer que les actifs d'information sensibles sont sécurisés (données financières, intellectuelles, personnelles et comportementales), qu'il s'agisse de données de première main ou secondaires.
- Les accords de Bâle définissant la notion de risque opérationnel, les **accords de Bâle 3** publiés en décembre 2010 visent à garantir un niveau minimum de capitaux propres et renforcer la solidité financière des banques.
- Dans la continuité de sa Loi de programmation militaire, l'état Français a mis en place la **Sécurisation des Opérateurs d'Importance Vitale (OIV)** en identifiant des secteurs et des entreprises vitales pour le maintient de l'activité du pays qui ont l'obligation, depuis 2016, de mettre en place un plan de Sécurité SI en collaboration avec l'ANSSI. Cela touche l'Energie, le Transport, les Communications, les Banques…

ISO2700 / Bâle 3 / OIV / SRI / DSP2 / RGPD / DSP2

- La Directive concernant la **Sécurité des Réseaux et de l'Information SRI (Network and Information System Security NIS),** entrée en vigueur en août 2016, a pour objectif de renforcer les capacités de cybersécurité des infrastructures critiques de l'UE. Pour cela, elle impose des obligations de sécurité et de notification des incidents à de nombreux types de fournisseurs de services essentiels et numériques, et exige notamment des États membres qu'ils adoptent des stratégies de cybersécurité nationales et coopèrent entre eux.

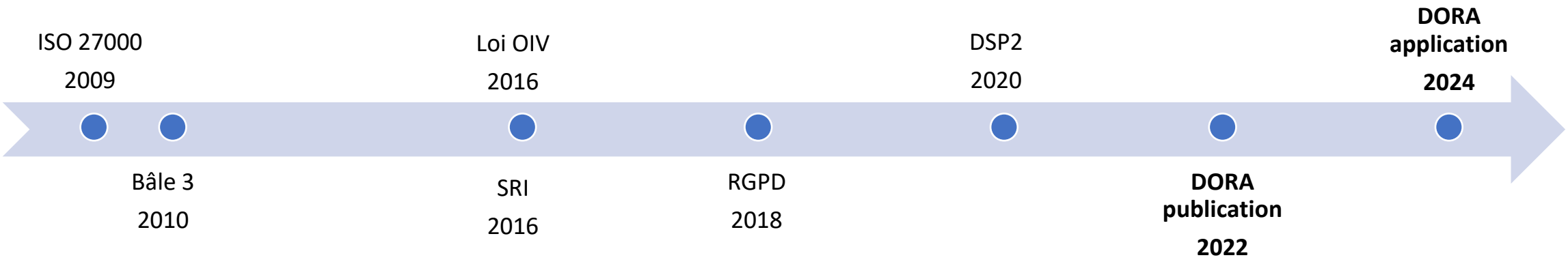
- Le **Règlement Général sur la Protection des données (RGPD)**, entré en application en mai 2018, renforce les droits des citoyens de l'Union Européenne et concerne tous les organismes publics et privés collectant ou traitant des données personnelles. Un consentement sur la collecte et le traitement des données doit être émis. Les entités qui collectent et traitent ces données personnelles sont juridiquement responsables en cas de fuite ou d'usage abusif.

- La deuxième **Directive européenne sur les Services de Paiement** (DSP2), en vigueur en Décembre 2020, comporte un ensemble de dispositions règlementaires visant à encadrer la prestation des services de paiements et renforcer la sécurité des paiements à l'échelle européenne. Les deux principaux domaines affectés par la DSP2 sont l'authentification des clients et l'accès des tiers aux comptes clients.

DORA – Les principes généraux

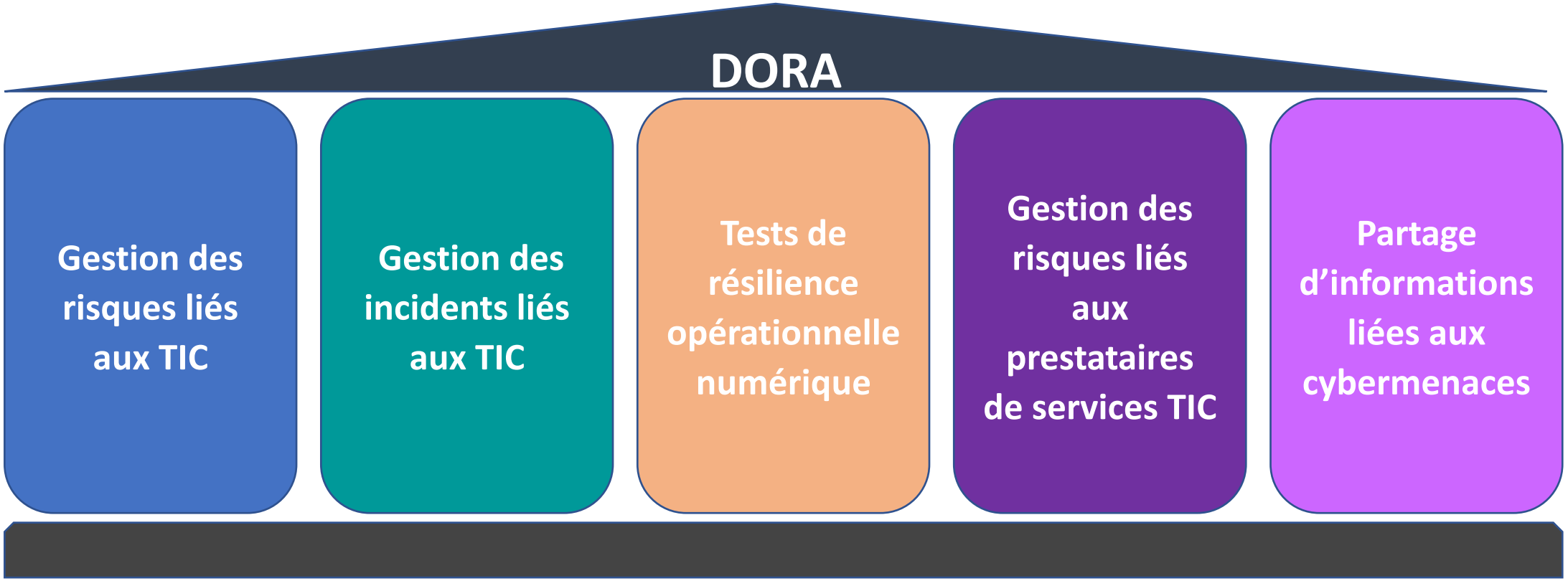
- L'absence de règles détaillées et exhaustives sur la résilience opérationnelle numérique au niveau de l'Union Européenne et le manque de coordination entre les initiatives nationales ont engendré des incohérences, des exigences redondantes et des coûts administratifs et de mise en conformité élevés pour les entités financières.
  Cette situation fragmente le marché unique, compromet la stabilité et l'intégrité du secteur financier de l'UE et porte atteinte à la protection des consommateurs et des investisseurs.

  - La Commission Européenne a publié la **Digital Operational Resilience Act (DORA)** en novembre 2022 pour une mise en application sous deux ans :



DORA – Les principes généraux

Le projet de règlement de la Commission européenne **Digital Operational Resilience Act (DORA)**, a pour objectif d'établir un cadre global pour les institutions financières de l'Union Européenne pour permettre d'unifier la gestion des risques liés aux **Technologies de l'Information et de la Communication (TIC).**
Il s'articule autour de cinq piliers :

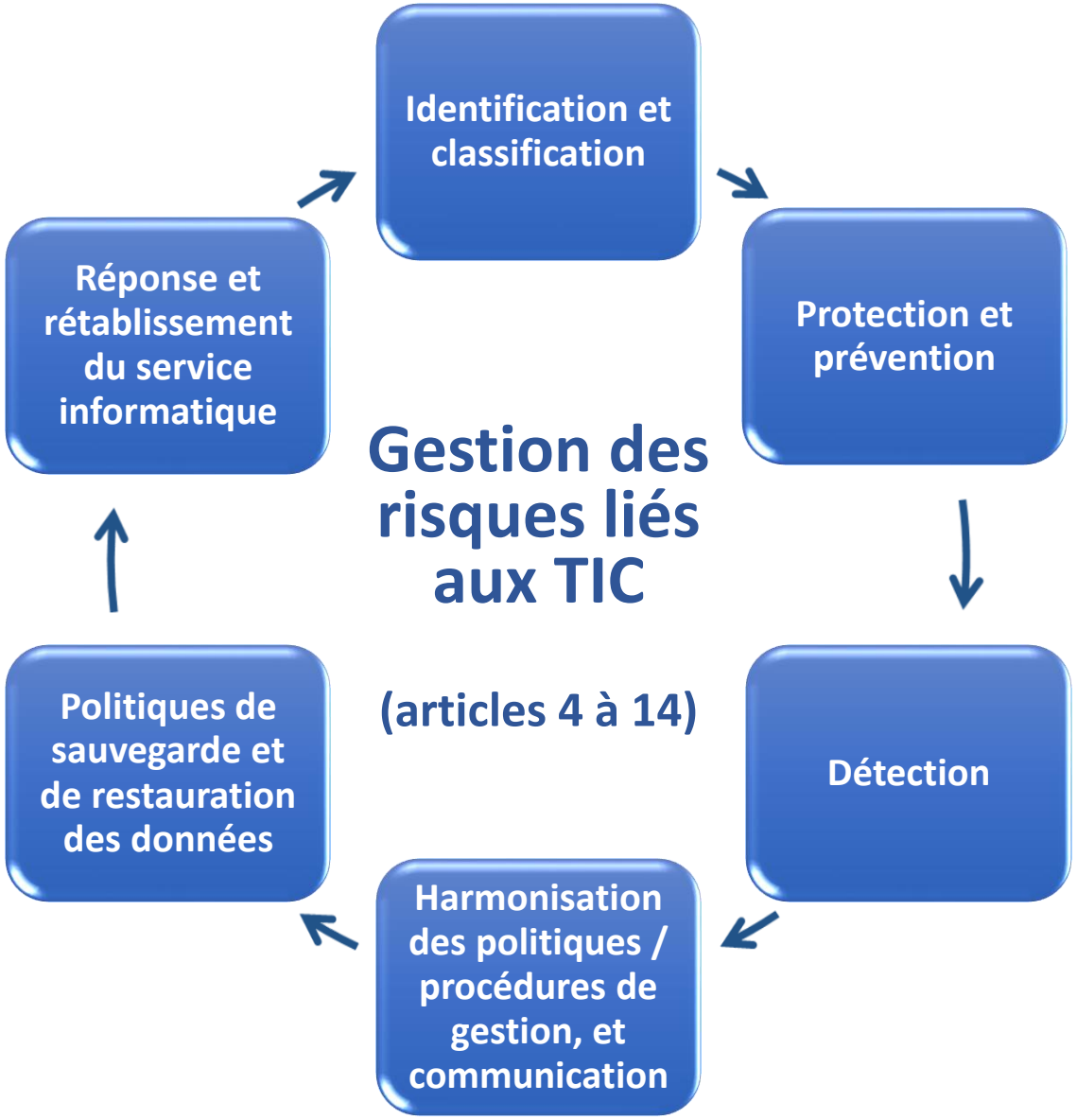


DORA – Les principes généraux

- Ce règlement sera appliqué dans les 27 pays membres de l'UE et concerne tous les professionnels du secteur financier appartenant ou ayant des opérations dans l'UE
- Ainsi que les prestataires de TIC considérés comme critiques

Les entités financières visées par DORA		
Les établissements de crédit	Les plateformes de négociation	Les institutions de retraite professionnelle
Les établissements de paiement	Les référentiels centraux	Les agences de notation de crédit
Les établissements de monnaie électronique	Les gestionnaires de fonds d'investissement alternatifs	Les contrôleurs légaux des comptes et les cabinets d'audit
Les entreprises d'investissement	Les sociétés de gestion	Les administrateurs d'indices de référence d'importance critique
Les prestataires de services sur cryptoactifs, les émetteurs de cryptoactifs, les émetteurs de jetons	Les prestataires de services de communication de données	Les prestataires de services de financement participatif
Les dépositaires centraux de titres	Les entreprises d'assurance et de réassurance	Les référentiels de titrisation
Les contreparties centrales	Les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire	Les tiers prestaires de services informatiques

DORA – Les cinq piliers



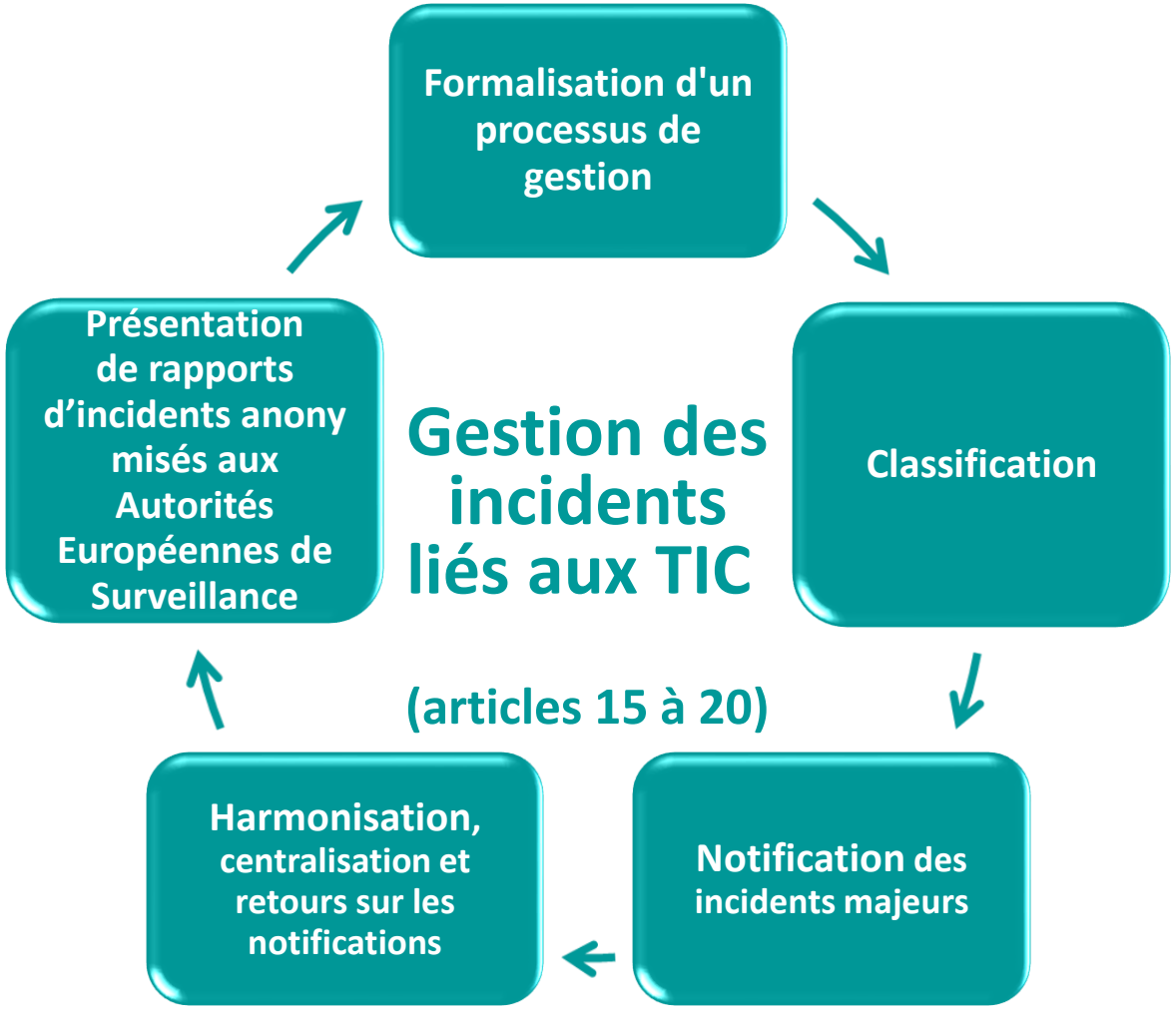
Objectif : veiller à ce que des mesures et des contrôles spécifiques soient mis en place pour limiter les perturbations du marché et des consommateurs causées par les incidents.

Exigences :

- Respecter les principes de Gouvernance en matière de risques liés aux TIC, en mettant l'accent sur la responsabilité de l'organe de gestion. Les Organisations concernées devront identifier leur tolérance au risque TIC, en fonction de leur appétit pour le risque et de leur tolérance aux impacts des perturbations des TIC.
- Mettre en place des processus et des mesures d'amélioration continue ainsi qu'une stratégie de communication de crise avec des rôles et des responsabilités clairs.

Défi : former obligatoirement l'organe de gestion et l'ensemble du personnel sur la résilience opérationnelle numérique.

DORA – Les cinq piliers



Objectif : harmoniser et centraliser la notification des incidents pour permettre au régulateur de réagir rapidement afin d'éviter la propagation de l'impact, et pour promouvoir l'amélioration de la connaissance collective des entreprises des menaces actuelles sur le marché.

Exigences :

- Standardiser la classification des incidents avec un ensemble de critères et seuils spécifiques (nombre d'utilisateurs touchés, durée, répartition géographique, perte de données, gravité de l'impact sur les systèmes TIC, criticité des services touchés, impact économique).
- Signaler les incidents majeurs à l'autorité de régulation dans le même jour ouvrable, selon un certain modèle. Un rapport de suivi sera également requis après une semaine, puis un mois. Ces rapports seront tous anonymisés, compilés et communiqués régulièrement à l'ensemble de la Communauté.

Défi :

- Adapter la méthode de classification des incidents pour se conformer aux exigences.
- Mettre en place les processus et les canaux appropriés pour pouvoir informer rapidement l'autorité de régulation en cas d'incident majeur.

DORA – Les cinq piliers

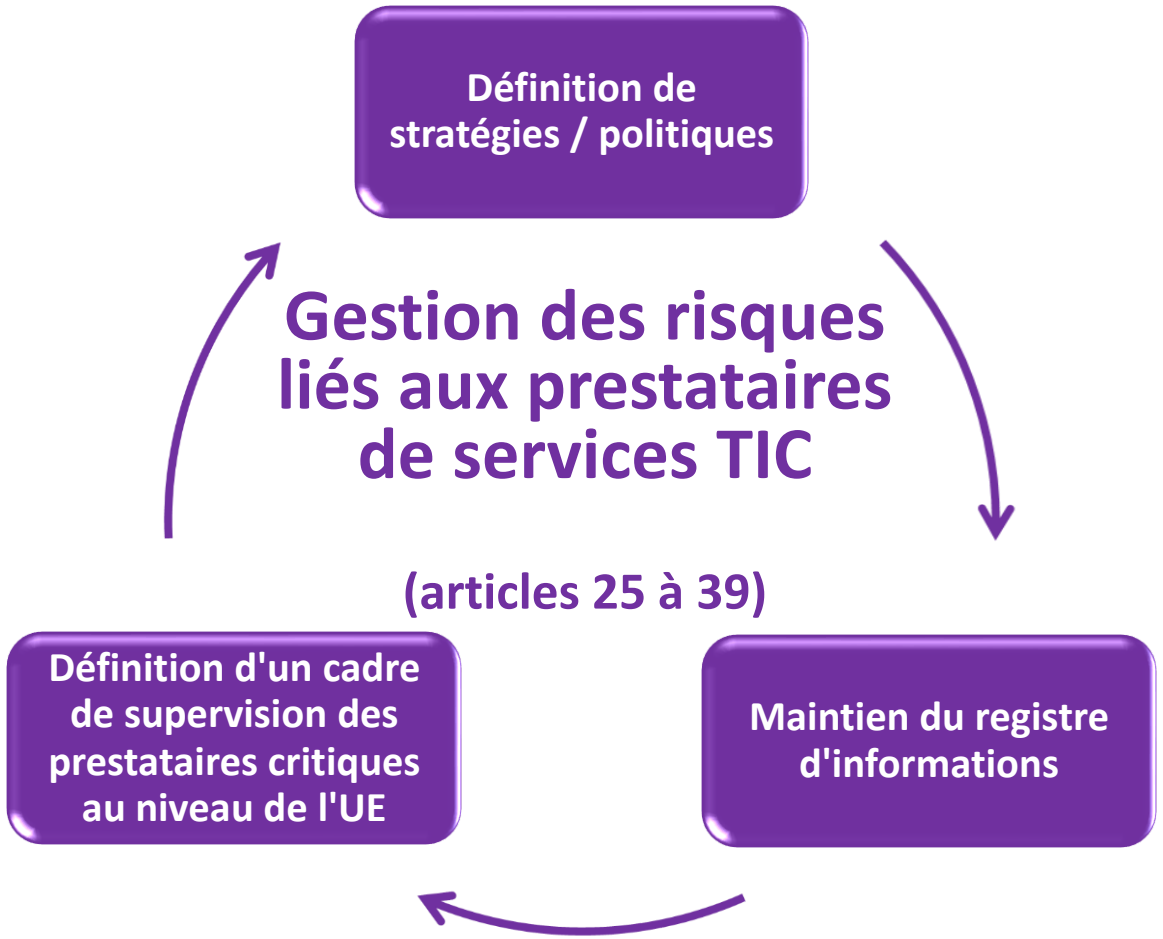
Objectif : tester l'efficacité du cadre de gestion des risques et les mesures en place pour répondre à un large éventail de scénarios d'incidents liés aux TIC.

Exigences :

- Mettre en place un programme complet de tests, en mettant l'accent sur les tests techniques.
- Pour les entreprises les plus critiques, organiser tous les trois ans un test de pénétration en direct à grande échelle, réalisé par des testeurs indépendants, couvrant les fonctions et services critiques et impliquant des tiers du secteur des TIC basés dans l'UE.
  - Approbation en amont du scénario par l'autorité de régulation
  - Réception d'un certificat de conformité à l'issue du test

Défi : se préparer efficacement à ces tests, et y impliquer les tiers critiques dans le domaine des TIC.

DORA – Les cinq piliers



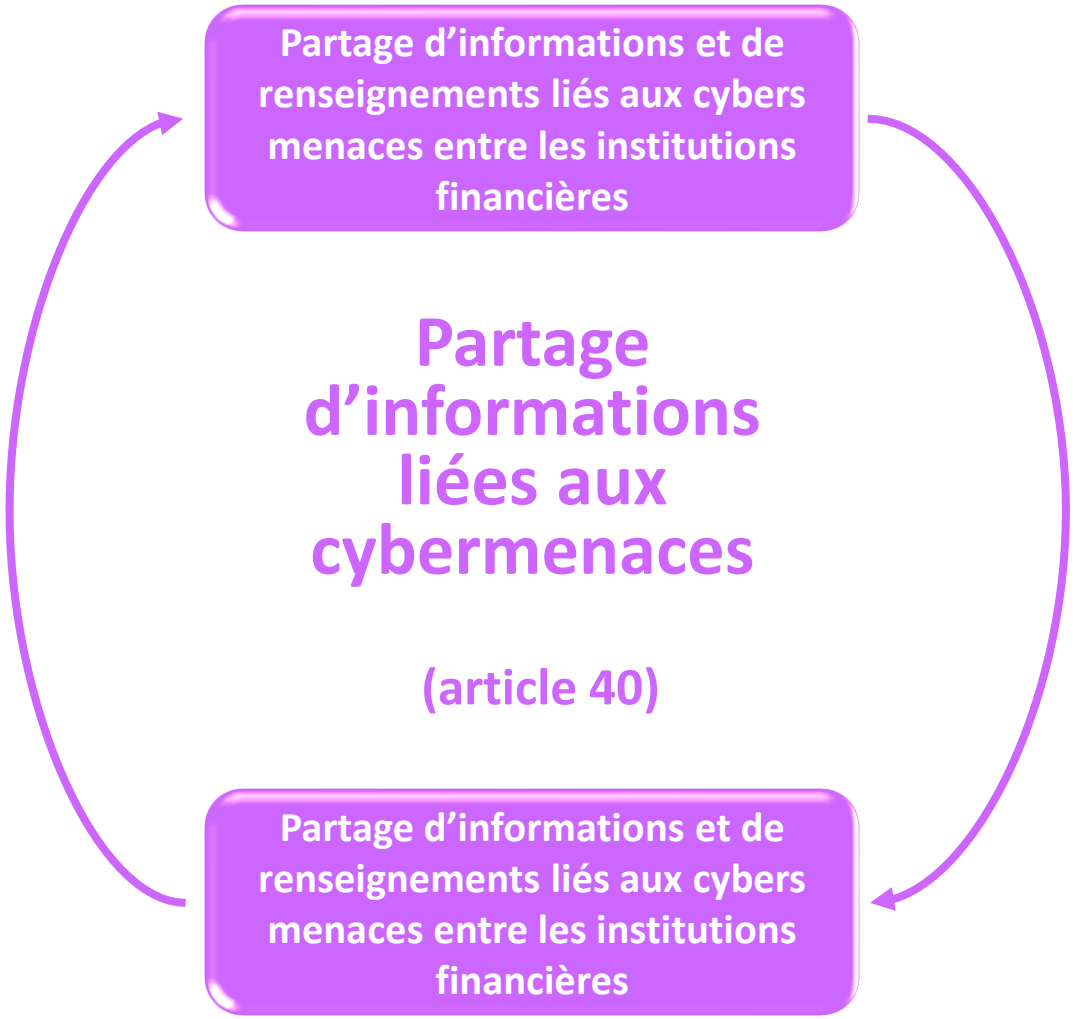
Objectif : contrôler et surveiller de manière appropriée les tiers TIC, en particulier ceux qui sous-tendent les fonctions critiques et essentielles pour le marché.

Exigences :

- Etablir un registre standard d'informations contenant la vue complète de tous les fournisseurs tiers de TIC, ainsi que les services qu'ils fournissent et les fonctions qu'ils sous-tendent.
- Surveiller les fournisseurs essentiels dans le cadre d'évaluations annuelles directement par le régulateur, avec sanctions en cas de non-conformité.
- Evaluer les fournisseurs de services TIC en fonction de certains critères avant de conclure un contrat (niveau de sécurité, risque de concentration, risques de sous-traitance), ainsi qu'une stratégie de sortie en cas de défaillance d'un fournisseur.

Défi : rassembler des informations sur tous les fournisseurs de TIC, tâche complexe pour les grandes organisations financières qui dépendent généralement de milliers de petits et grands fournisseurs et de systèmes de gestion de contrats hérités qui rendent difficile l'extraction de données.

DORA – Les cinq piliers



Objectif : promouvoir l'échange d'informations et de renseignements sur les cybermenaces entre les organismes financiers afin de leur permettre d'être mieux préparés.

Exigence :

- Mettre en place des accords de partage d'informations anonymisées entre entreprises du secteur financier pour les cybermenaces.
- Informer l'autorité de régulation.

Défi :

- Maintenir les accords déjà mis en place.
- Rendre visibles les initiatives pour encourager un plus grand nombre d'entreprises à y participer.

Impact pour les prestataires de services

Impact pour les ESN

DORA concerne donc également les tiers prestataires de services informatiques tout en ne réduisant en aucun cas les responsabilités des établissements financiers.

- Les tiers fournisseurs TIC devront identifier s'ils sont considérés comme critiques sur la base de critères réglementaires tels que le nombre et le caractère systémique des entités financières qui en dépendent ainsi que son degré de substituabilité.
- Chaque prestataire de services TIC critique sera contrôlé par une autorité de supervision qui évaluera si le prestataire de services a mis en place les dispositifs adéquats de maîtrise des risques liés aux TIC pouvant impacter les institutions financières (article 37).
- L'autorité compétente pourra procéder à des contrôles sur pièces ou sur place (articles 33 à 35) et aura également le pouvoir de prononcer des sanctions en cas de non-conformité. Celles-ci peuvent notamment être des pénalités financières et des astreintes journalières à un taux de 1% du chiffre d'affaires mondial de la précédente année d'exercice réalisé par le prestataire de services TIC concerné, et ce pendant une période totale de 6 mois maximum (article 311).
- Des clauses contractuelles obligatoires doivent être mises en place entre l'établissement financiers et les prestataires de Service. Le régulateur pourra demander aux établissements financiers de mettre fin à leurs accords avec un prestataire.

Impact pour les ESN

Tôt ou tard, les établissements financiers travaillant avec des ESN vont leur demander d'être en accord avec la Règlementation DORA.

- Les consultants des ESN seront directement impactés durant leur mission pour des établissements financiers
- Les ESN devront elles-mêmes gérer leur SI au siège selon DORA
- Les ESN devront vérifier que leur propres tierces parties sont en accord avec DORA

DORA s'inspire de ISO 27000

La démarche de mise en conformité avec DORA est en convergence avec l'application de la norme ISO 27000.

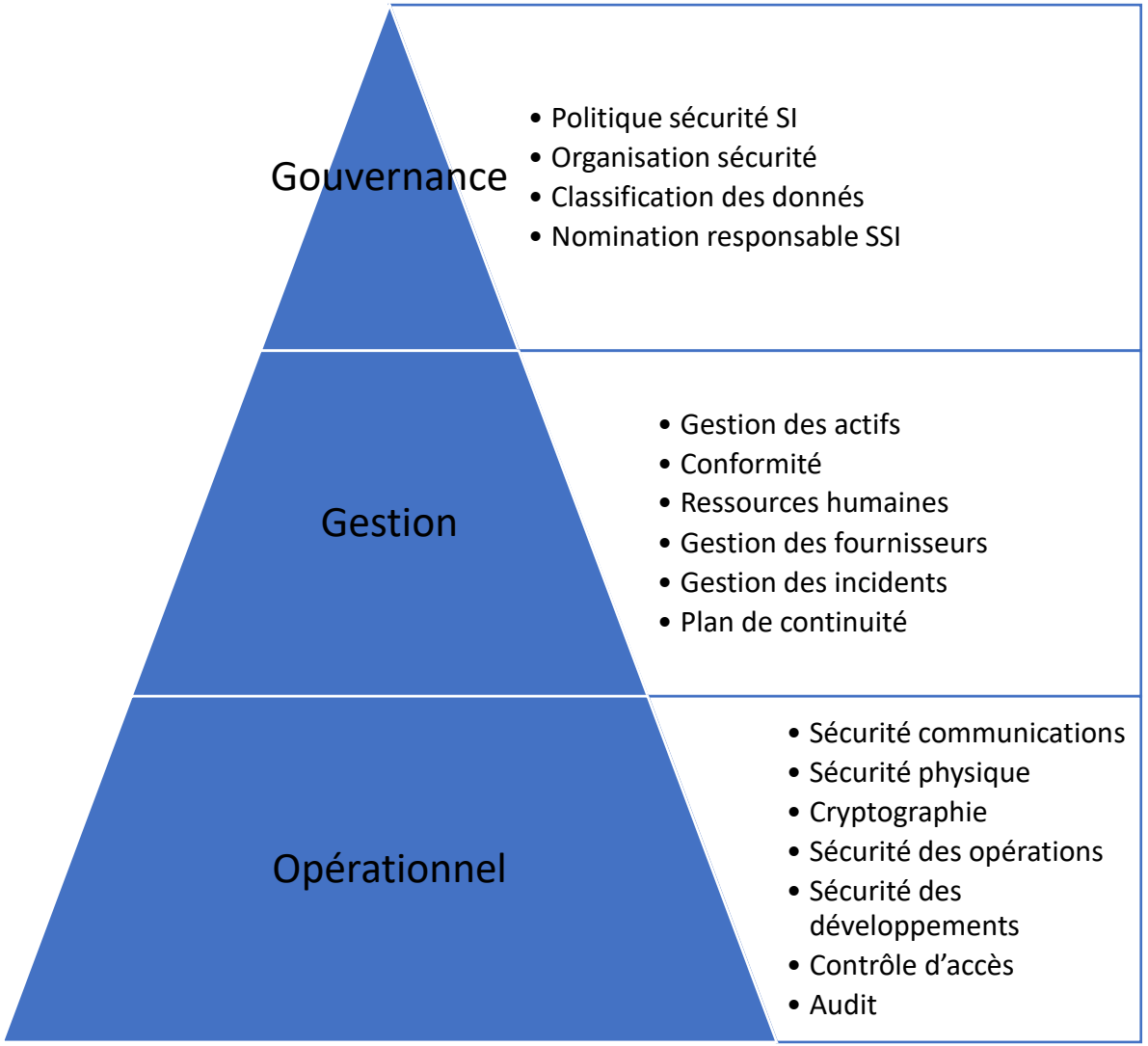
La norme ISO 27002 se découpe en :

- 4 thèmes : Contrôles de l'organisation, Contrôles des personnes, Contrôles physiques, Contrôles techniques.
- 14 chapitres.
- 114 mesures de sécurité.

Pour une ESN cela implique de :

1. Désigner un responsable SI et un responsable RSSI.
2. Mettre en place une gouvernance impliquant la direction de l'entreprise.
3. Qualifier les composants du système d'information : confidentialité, criticité, vulnérabilité.
4. Former à la sécurité SI, revoir les contrats ou règlements internes.
5. Durcir le système d'information avec des fonctions d'audit, de filtrage, de tolérances aux pannes.

➔ **L'objectif n'est pas d'être certifié ISO 27000 mais d'utiliser ce cadre pour répondre aux attentes des entités financières.**



ANNEXES

Acteurs impactés par DORA

DORA - Article 2 - Personal scope

1. Without prejudice to paragraphs 3 and 4, this Regulation applies to the following entities:
   - (a) credit institutions,
   - (b) payment institutions, including payment institutions exempted in accordance with Article 32 (1) of Directive (EU) 2015/2366,
   - (ba) account information service providers,
   - (c) electronic money institutions, including electronic money institutions exempted in accordance with Article 9 (1) of Directive 2009/110/EC,
   - (d) investment firms,
   - (e) crypto-asset service providers as authorized under MiCA and issuers of assets-referenced tokens,
   - (f) central securities depositories,
   - (g) central counterparties,
   - (h) trading venues,
   - (i) trade repositories,
   - (j) managers of alternative investment funds,

Acteurs impactés par DORA

- (k) management companies,
- (l) data reporting service providers, PE734.260v01-00 58/173 AG\1259083EN.docx EN
- (m) insurance and reinsurance undertakings,
- (n) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries,
- (o) institutions for occupational retirement provision,
- (p) credit rating agencies,
- (r) administrators of critical benchmarks,
- (s) crowdfunding service providers,
- (t) securitisation repositories,
- (u) ICT third-party service providers.

2. For the purposes of this Regulation, entities referred to in paragraph (a) to (t) shall collectively be referred to as ‘financial entities’.

Acteurs impactés par DORA

3. This Regulation shall not apply to:

- (a) managers of alternative investment funds referred to in Article 3(2) of Directive 2011/61/EU;
- (b) insurance and reinsurance undertakings referred to in Article 4 of Directive 2009/138/EC;
- (c) institutions for occupational retirement provision which operate pension schemes which together do not have more than 15 members in total;
- (d) natural or legal persons exempted from the application of Directive 2014/65/EU pursuant to Articles 2 and 3 of that Directive; AG\1259083EN.docx 59/173 PE734.260v01-00 EN
- (e) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries which are microenterprises, small or medium-sized enterprises;
- (g) institutions referred to in point (3) of Article 2(5) of Directive 2013/36/EU.

Acteurs impactés par DORA

4. Member States may exempt institutions referred to in points (4) to (23) of Article 2(5) of Directive 2013/36/EU that are located within their respective territory from the scope of this Regulation. In case such option is exercised, this Regulation shall not apply to the exempted institutions.

   Where a Member State makes use of such option, it shall inform the Commission thereof as well as of any subsequent changes. The Commission shall make the information public on a website or other easily accessible means.

Une synthèse

Source : [Explorons DORA ! - Almond]

	Gestion des risques liés aux (TIC) (articles 4 à 14)	Gestion, classification et notification des incidents liés à l'informatique ; (articles 15 à 20)	Tests de résilience opérationnelle numérique (articles 21 à 24)	Gestion des risques liés aux tiers prestataires de services informatiques (articles 25 à 39)	Partage d'informations (article 40)
Objectifs visés par DORA à travers ces piliers	• mettre en place et maintenir des systèmes et des outils informatiques résilients afin de réduire au minimum l'incidence des risques informatiques, • identifier les sources de risques informatiques et adopter des mesures de protection et de prévention, • de détecter rapidement les activités anormales, • instaurer des politiques de continuité des activités et des plans de rétablissement après sinistre	• assurer une surveillance, un traitement et un suivi cohérents et intégrés des incidents liés à l'informatique, afin de déterminer et de supprimer les causes profondes pour éviter que de tels incidents ne se (re)produisent.	• évaluer l'état de préparation en cas d'incidents liés à l'informatique, recenser les faiblesses, les défaillances ou les lacunes en matière de résilience opérationnelle numérique afin d'être en mesure de mettre rapidement en œuvre des mesures correctives.	• permettre un suivi complet, par l'entité financière, du risque associé aux tiers prestataires de services informatiques tout au long des différentes étapes de leur relation, à savoir la conclusion du contrat, son exécution, sa résiliation et la phase post-contractuelle.	• Sensibiliser au risque informatique et renforcer les capacités défensives des entités financières et leurs techniques de détection des menaces grâce aux échanges des informations et des renseignements sur les cybermenaces.
Articles par pilier	• ***Art 4*** *: Gouvernance et organisation* • ***Art 5*** *: Cadre de gestion des risques informatiques* • ***Art 6*** *: Systèmes, protocoles et outils informatiques* • ***Art 7*** *: Identification* • ***Art 8*** *: Protection et prévention* • ***Art 9*** *: Détection* • ***Art 10*** *: Réponse et rétablissement* • ***Art 11*** *: Politiques de sauvegarde et méthodes de rétablissement* • ***Art 12*** *: Apprentissage et évolution* • ***Art 13*** *: Communication* • ***Art 14*** *: Harmonisation accrue des outils, méthodes, processus et politiques de gestion des risques informatiques*	• ***Art15*** *: Processus de gestion des incidents liés à l'informatique* • ***Art 16*** *: Classification des incidents liés à l'informatique* • ***Art 17*** *: Notification des incidents majeurs liés à l'informatique* • ***Art 18*** *: Harmonisation du contenu et des modèles des rapports de notification* • ***Art 19*** *: Centralisation des notifications d'incidents majeurs liés à l'informatique* • ***Art 20*** *: Retour d'information en matière de surveillance*	• ***Art 21*** *: Exigences générales applicables à la réalisation de tests de résilience opérationnelle numérique* • ***Art 22*** *: Test des outils et systèmes informatiques* • ***Art 23*** *: Tests avancés d'outils, de systèmes et de processus informatiques sur la base de tests de pénétration fondés sur la menace* • ***Art 24*** *: Exigences applicables aux testeurs*	❑ ***SECTION 1*** *: Principes clés pour une bonne gestion des risques liés aux tiers prestataires de services informatiques* • ***Art 25*** *: Principes généraux* • ***Art 26*** *: Évaluation préliminaire du risque de concentration informatique et autres accords de sous-traitance* • ***Art 27*** *: Principales dispositions contractuelles* ❑ ***SECTION 2*** *: Cadre de supervision des tiers prestataires critiques de services informatiques* • ***Art 28*** *: Désignation de tiers prestataires critiques de services informatiques* • ***Art 29*** *: Structure du cadre de supervision* • ***Art 30*** *: Tâches du superviseur principal* • ***Art 31*** *: Pouvoirs du superviseur principal* • ***Art 32*** *: Demande d'informations* • ***Art 33*** *: Enquêtes générales* • ***Art 34*** *: Inspections sur place* • ***Art 35*** *: Supervision continue* • ***Art 36*** *: Harmonisation des conditions permettant l'exercice de la supervision* • ***Art 37*** : Suivi par les autorités compétentes • ***Art 38*** *: Redevances de supervision* • ***Art 39*** *: Coopération internationale*	• ***Art 40*** *: Dispositifs de partage d'informations et de renseignements sur les cybermenaces*