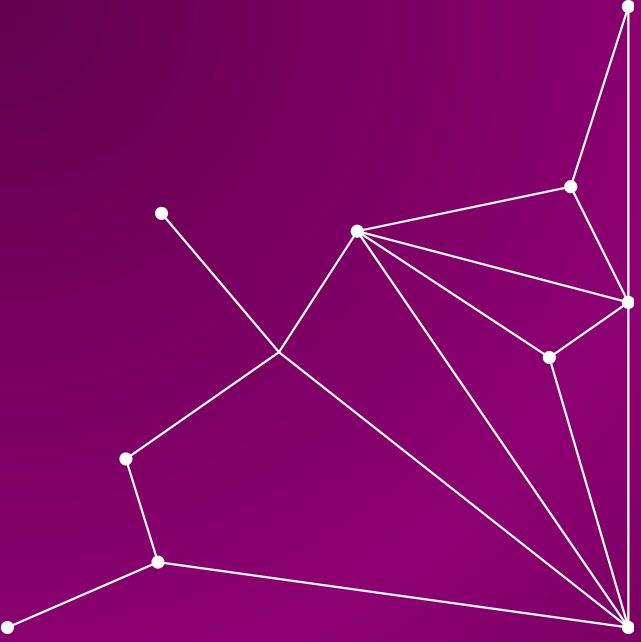


CONFORMITÉ DORA PAR L'AUTOMATISATION ET L'OCHESTRATION

Smartbot Consulting

Smartbot Consulting

Table des matières

Introduction 01
DORA en chiffres

Thèmes clés et objectifs de DORA 04

Stratégies d'automatisation pour la conformité DORA : Transformer la directive en opportunité 05

Technologies clés pour la mise en œuvre : l'ingénierie de la résilience numérique 07

Détails spécifiques des règlements délégués et d'exécution 09

Champ d'application de DORA 10

Supervision et sanctions 10

Implications et perspectives 10

Étapes de transformation : un voyage méthodologique 11

Points importants supplémentaires 12

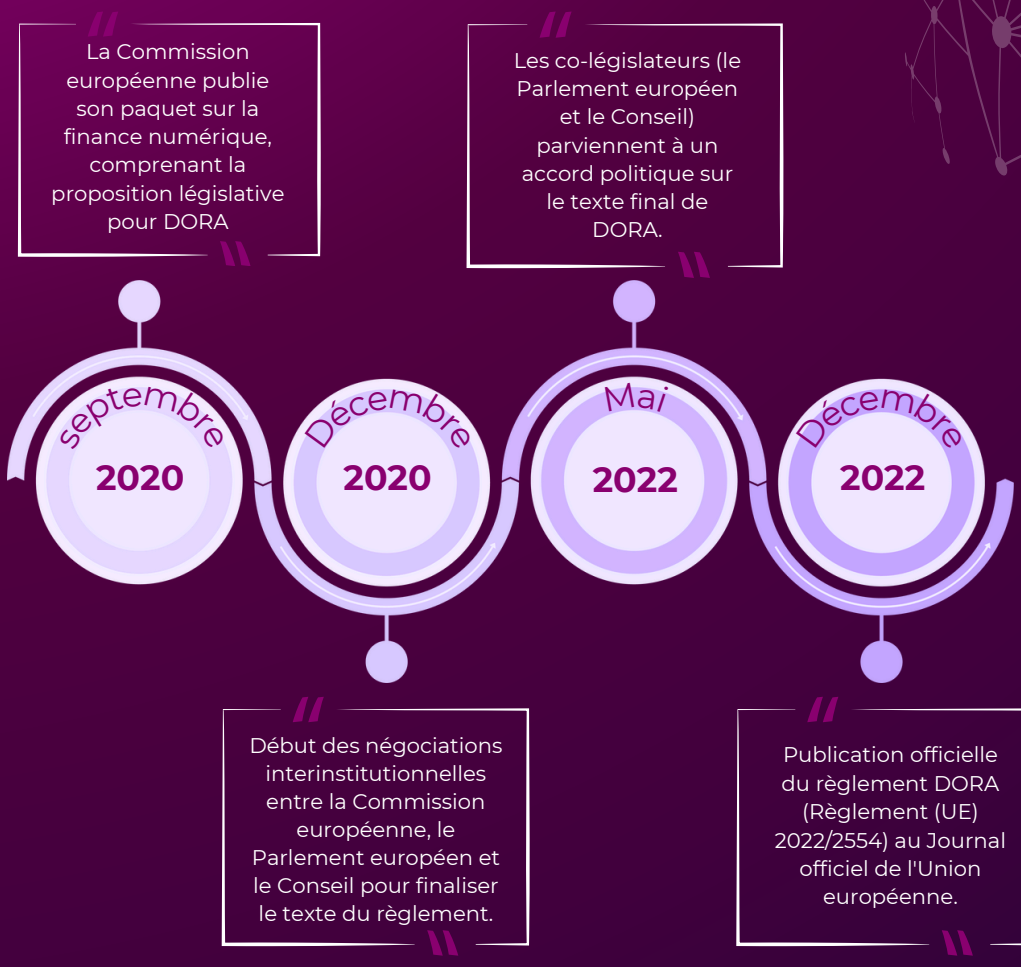
Conclusion : DORA - une transformation au-delà de la conformité réglementaire 13

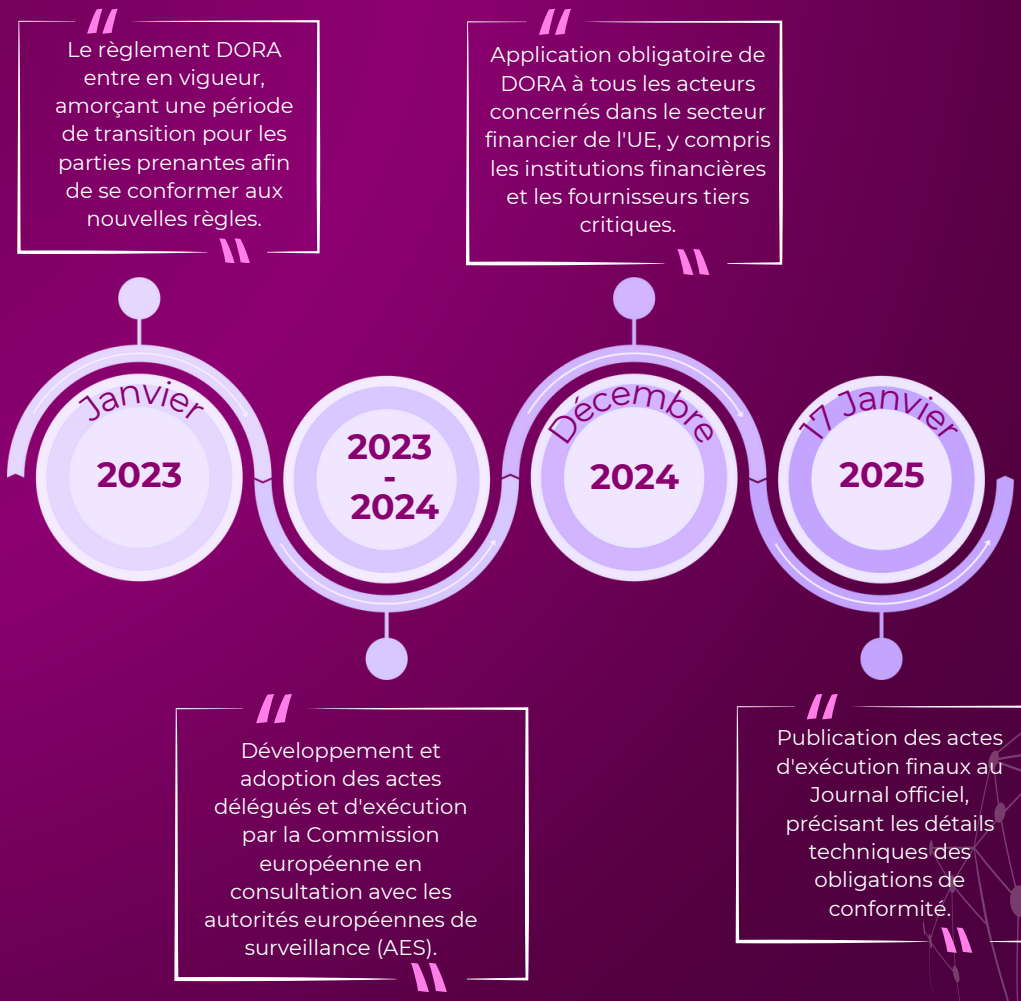
Références et Définitions clés 15

FAQ 16

1. Introduction

Dans un environnement numérique en constante évolution, le secteur financier est confronté à des défis sans précédent pour maintenir une résilience opérationnelle robuste. La sophistication croissante des cybermenaces, combinée à la dépendance du secteur envers des systèmes informatiques complexes, nécessite une approche proactive et stratégique de la sécurité. L'Union européenne a mis en place le Règlement sur la résilience opérationnelle numérique (DORA), Règlement (UE) 2022/2554, une législation clé conçue pour répondre à ces défis. Ce règlement vise à renforcer la capacité du secteur financier à prévenir, gérer et récupérer des incidents liés aux technologies de l'information et de la communication (TIC). Ce livre blanc élaboré par Smartbot Consulting, est un guide pour les décideurs et les professionnels de la transformation numérique, offrant une feuille de route complète pour naviguer dans les complexités de la conformité à DORA.

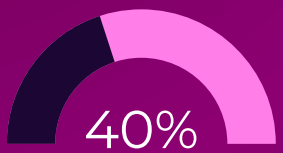




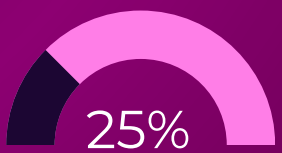
Au lieu de considérer DORA comme une simple obligation réglementaire, les institutions financières devraient y voir **une opportunité stratégique** de transformation. En adoptant les exigences de DORA, les organisations peuvent améliorer leur infrastructure technologique, protéger les données sensibles des clients, maintenir la confiance des parties prenantes et atténuer les risques financiers et réputationnels potentiels. Ce livre blanc met en évidence le potentiel de DORA pour devenir un avantage concurrentiel, en soulignant l'importance de la résilience numérique comme une priorité commerciale fondamentale. Il explorera les aspects critiques du règlement, tels que **le signalement des incidents**, les **tests de résilience opérationnelle numérique** et la **gestion des risques liés aux TIC.** De plus, ce document se penchera sur l'importance stratégique de **l'automatisation** et de l'**orchestration** des processus pour atteindre une conformité efficace et efficiente. En offrant des approches pratiques et des meilleures pratiques, ce livre blanc a pour objectif d'aider les entités financières à dépasser la simple conformité, en utilisant DORA comme un catalyseur pour réinventer la résilience et stimuler l'amélioration de la performance opérationnelle. En fin de compte, ce document est conçu pour transformer le cadre DORA d'une contrainte en un levier de transformation et de différenciation.

Dora en chiffres

Répartition du coût moyen de mise en conformité DORA
(1,2 à 3,5 millions d'euros par organisation)

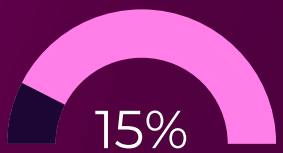


Infrastructure technologique



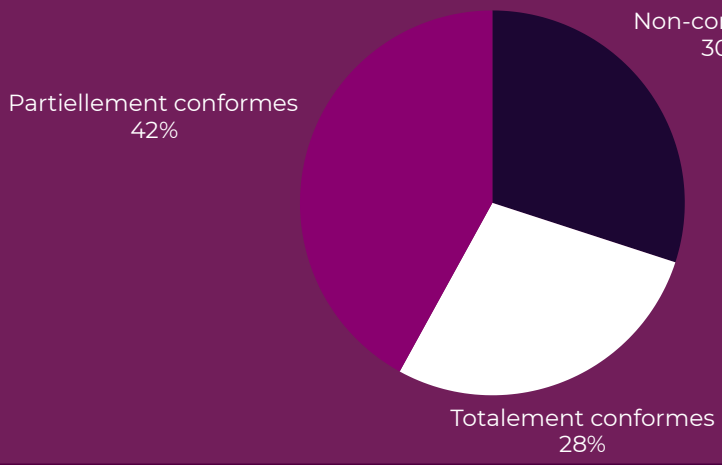
Formation et compétences

Outils de monitoring



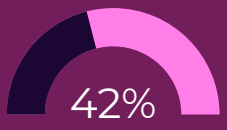
Conseil et accompagnement

Niveau de conformité Européen

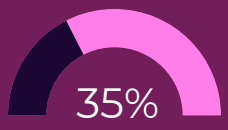


Evolution du marché de la résilience numérique

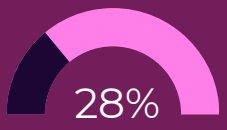
2023 : 12.5 milliard d'euro
Projection 2026 : 24,3 milliard d'euro



Cloud et solutions hybrides



Automatisation



IA et Machine learning

2. **Thèmes clés et objectifs de DORA**

- **Approche holistique de la résilience numérique :** DORA dépasse les mesures réactives pour mettre l'accent sur une approche proactive et préventive de la gestion des risques technologiques. Par exemple, Au lieu d'attendre qu'un incident se produise, une institution financière mettrait en place un processus de **cartographie complète** de son infrastructure IT, afin d'identifier tous les points faibles potentiels.
- **Champ d'application élargi :** DORA s'applique à un large éventail d'entités financières, y compris les banques, les sociétés d'investissement, les assureurs, les gestionnaires d'actifs, les plateformes de financement participatif, les émetteurs de monnaie électronique, les prestataires de services de paiement, ainsi que les fournisseurs tiers de services TIC.
- **Concentration sur les risques liés aux fournisseurs tiers de TIC :** Un aspect significatif de DORA est son accent sur la gestion des risques associés à la dépendance envers des prestataires externes de services TIC. Cela inclut l'évaluation, le suivi et la gestion des risques posés par ces fournisseurs.
- **Harmonisation des exigences :** DORA vise à harmoniser les éléments contractuels clés et les exigences relatives aux prestataires tiers de services TIC afin d'assurer une surveillance et une gestion des risques cohérentes à travers l'UE.

3. Stratégies d’automsatisation pour la conformité DORA : Transformer la directive en opportunité

L’automatisation comme levier de résilience

Dans l'écosystème réglementaire imposé par DORA, l'automatisation n'est plus une option, mais une nécessité stratégique. Elle permet de transformer les exigences complexes en processus dynamiques et intelligents.

Eléments clés des règlements

- **Gestion des risques TIC** : Les institutions financières doivent établir des cadres complets de gestion des risques TIC, incluant la cartographie des systèmes, l'identification des vulnérabilités et la mise en œuvre de stratégies d'atténuation.
- **La cartographie des systèmes TIC** représente le socle fondamental de la conformité DORA. Il s'agit de créer une vision holistique et dynamique du système d'information.
  - Approche méthodologique :
    - Utilisation d'outils de découverte automatique
    - Identification des dépendances inter-applicatives
    - Création de référentiels de configuration dynamiques
  - **Technologies clés :**
    - Outils CMDB (Configuration Management Database)
    - Solutions de découverte automatique basées sur les logs « Process mining »
    - Plateformes d'intelligence artificielle pour la modélisation des systèmes

- **Rapport des incidents TIC** : Les entités financières doivent disposer de processus pour signaler les incidents majeurs liés aux TIC aux autorités compétentes. Les règlements spécifient des délais de déclaration et exigent des modèles standardisés.
  - **Composantes principales :**
    - Monitoring en temps réel
    - Détection des anomalies
    - Évaluation prédictive des risques
    - Tableaux de bord dynamiques

- **Tests de résilience opérationnelle numérique :** Les entités financières seront soumises à des régimes de tests, y compris des tests de pénétration dirigés par des menaces (TLPT- Threat-Led Penetration Testing). DORA autorise les tests internes sous certaines conditions, mais exige que les renseignements sur les menaces pour un TLPT proviennent toujours d'un fournisseur externe. Comme le stipule le règlement 2022/2554 : « *(...) ce règlement doit permettre l'utilisation de testeurs internes pour effectuer des TLPT, à condition qu'il y ait une approbation de la supervision, aucune situation de conflit d'intérêts et une alternance périodique entre testeurs internes et externes (tous les trois tests), tout en exigeant que le fournisseur des renseignements sur les menaces soit toujours externe à l'entité financière.* »

- **Modalités d'automatisation :**
  - Scénarios de simulation avancés
  - Tests de pénétration automatisés
  - Génération dynamique de scenarii de risques
  - Analyse comparative automatique
  - évaluation continue et automatisée des fournisseurs tiers,
  - Gestion contractuelle intelligente,
  - Registre d'informations dynamique

- **Technologies clés :** une plateforme intégrée de gestion des risques et des fournisseurs comme ROK solution conçue pour :
  - automatiser les supervison des fournisseurs, évaluer, gérer et suivre les contrats, assurer une visibilité accrue et une gestion efficace des risques associés aux fournisseurs tiers.

- **Supervision des fournisseurs tiers critiques de services TIC :** Les règlements introduisent un cadre de supervision pour les fournisseurs tiers critiques, basé sur des critères quantitatifs et qualitatifs pour déterminer les fournisseurs qui entrent dans cette catégorie.

- **Dispositions contractuelles :** Les entités financières doivent accorder une attention particulière aux dispositions contractuelles avec les fournisseurs tiers de services TIC et s'assurer qu'elles intègrent les clauses appropriées. Les règlements précisent également ce qui doit être inclus dans ces contrats et les informations à collecter sur les fournisseurs tiers.

- **Registre d'informations :** Les entités financières sont tenues de maintenir un registre d'informations (RoI) contenant des détails sur leurs contrats de services TIC, leurs dépendances et leurs actifs TIC.

4. **Technologie clés pour la mise en oeuvre :** l'ingénierie de la résilience numérique.

Le numérique comme un bouclier stratégique

Dans l'écosystème réglementaire de DORA, les technologies ne sont plus de simples outils, mais des architectes de la résilience organisationnelle. Elles transforment les contraintes réglementaires en opportunités stratégiques de performance et de différenciation.

Solutions de gestion des risques : cartographier l'invisble

L'ère des tableurs et des approches manuelles de gestion des risques appartient désormais au passé. Les nouvelles solutions sont des systèmes nerveux numériques, capables de détecter, analyser et prédire les menaces avant même leur émergence.

Caractéristiques révolutionnaires

- Détection prédictive des vulnérabilités
- Modélisation dynamique des scenarii de risques
- Évaluation continue en temps réel
- Intégration des données multi-sources

Technologies habilitantes

- Plateformes GRC (Gouvernance, Risque, Conformité)
- Solutions d'analyse de risques prédictifs
- Systèmes de notation dynamique des risques

Plateformes d'orchestration : synchroniser la complexité

L'orchestration devient l'art de transformer la complexité réglementaire en processus fluides et intelligents. Ces plateformes agissent comme des chefs d'orchestre technologiques, garantissant l'harmonie entre systèmes, règles et objectifs stratégiques.

Principes fondateurs

- Interconnexion des systèmes hétérogènes
- Workflows adaptatifs
- Gouvernance unifiée
- Traçabilité exhaustive

Références : L'Autorité Bancaire Européenne recommande des architectures d'orchestration capables de :

- Gérer la complexité réglementaire
- Assurer la résilience opérationnelle
- Faciliter le reporting

Outils d'automatisation des tests : la résilience par la simulation

Les tests ne sont plus des exercices formels, mais des simulations dynamiques et intelligentes. Ces outils transforment la conformité en une démarche proactive de transformation continue.

Modalités avancées

- Génération automatique de scenarii
- Tests de pénétration intelligents
- Simulation de crises numériques
- Analyse comparative automatisée

Intelligence Artificielle et Machine Learning : l'avenir de la conformité

L'IA et le machine learning transcendent la simple technologie pour devenir de véritables "systèmes nerveux" de la résilience numérique.

Capacités stratégiques

- Détection des anomalies
- Prédiction des risques émergents
- Apprentissage continu
- Recommandations stratégiques

Conclusion : au-delà de la technologie

Ces technologies ne sont pas de simples outils de conformité, mais des catalyseurs de transformation stratégique. Elles invitent les institutions financières à réinventer leur approche de la résilience numérique.

5. Détails spécifiques des règlements délégués et d'exécution

Règlement 2024/1773 : Ce règlement définit plusieurs facteurs clés que les entités financières doivent considérer lors de l'évaluation des risques liés à l'utilisation de fournisseurs tiers de services TIC, notamment :

- « le type de services TIC inclus dans l'accord contractuel »
- « la localisation du fournisseur tiers de services TIC »
- « la nature des données partagées avec le fournisseur tiers de services TIC »
- « la concentration des services TIC soutenant des fonctions critiques ou importantes sur un seul fournisseur tiers de services TIC ou sur un nombre restreint de ces fournisseurs »

Règlement 2024/1774 : Ce règlement met l'accent sur l'importance de la gestion des risques TIC résiduels, en particulier ceux qui dépassent le niveau de tolérance au risque d'une entité financière.

- Il exige l'élaboration d'un inventaire des risques TIC résiduels acceptés et des examens périodiques de ces risques.
- Il impose également aux entités financières de vérifier la manière dont les fournisseurs tiers de services TIC gèrent les vulnérabilités et de fournir des rapports ponctuels sur ces vulnérabilités, ainsi que des statistiques et des tendances.
- Ce règlement contient aussi des exigences sur la surveillance et la protection des données dans les environnements de préproduction, ainsi que sur la protection de l'intégrité des codes sources des systèmes TIC développés en interne ou par des tiers.
- Enfin, il fixe des exigences pour la surveillance des actifs TIC, y compris les besoins en capacité et les évaluations automatisées des vulnérabilités.

Règlement 2024/2956 : Ce règlement d'exécution établit des modèles standardisés pour le registre d'informations.

- Il fournit des définitions de termes clés tels que « chaîne d'approvisionnement des services TIC » et « rang » d'un tiers.
- Il impose la collecte d'informations sur les arrangements contractuels, les fournisseurs tiers de services TIC, ainsi que sur la chaîne d'approvisionnement des services TIC.
- Il insiste particulièrement sur la nécessité d'identifier « les entités utilisant les services TIC fournis par les fournisseurs tiers de services TIC ».
- Il détaille les modèles à utiliser pour rapporter ces informations, y compris : les informations sur les entités, les détails des arrangements contractuels (y compris la date de début, la date de fin et la loi applicable), les informations sur les fournisseurs tiers de services TIC, et les détails sur l'utilisation du service TIC.

6. Champ d'application de DORA

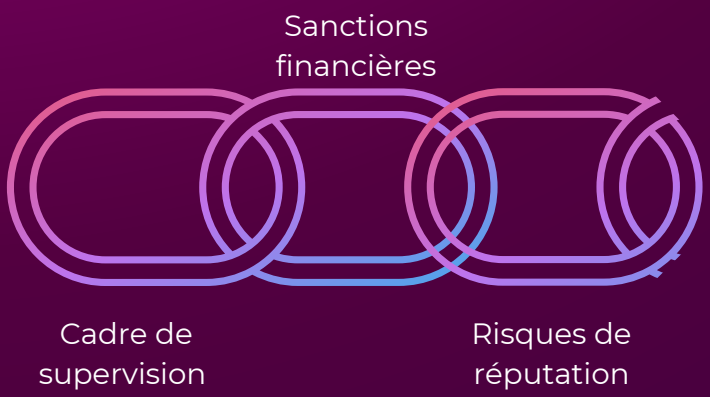
Entités concernées : DORA s'applique à une large gamme d'entités financières, notamment, mais sans s'y limiter :

- Institutions de crédit
- Établissements de paiement
- Fournisseurs de services d'information sur les comptes
- Établissements de monnaie électronique
- Sociétés d'investissement
- Fournisseurs de services liés aux crypto-actifs
- Fournisseurs de services de déclaration des données
- Entreprises d'assurance et de réassurance
- Fournisseurs tiers de services TIC

Entités exclues : DORA ne s'applique pas aux gestionnaires de fonds d'investissement alternatifs, aux petites compagnies d'assurance et aux très petites institutions de retraite professionnelle.

7. Supervision et sanctions

Cadre de supervision DORA



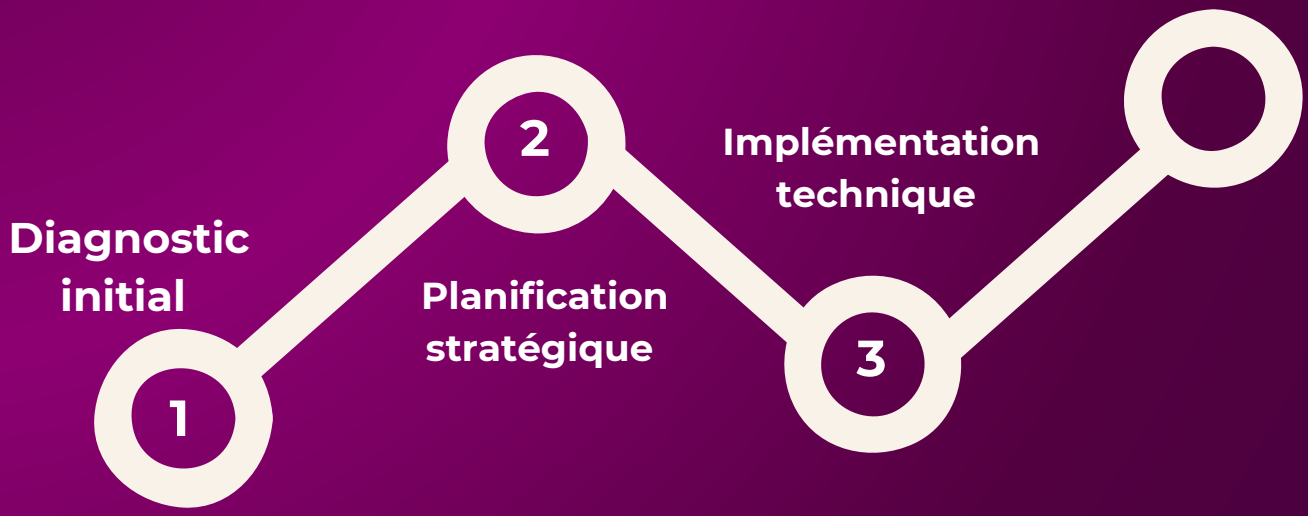
Cadre de supervision : Un nouveau cadre de supervision est introduit par DORA afin de prévenir les risques systémiques liés aux défaillances des fournisseurs de services TIC. Ce cadre s'applique aux fournisseurs tiers de services TIC considérés comme critiques.

- **Sanctions :** DORA prévoit des sanctions financières importantes en cas de non-conformité, avec des amendes pouvant atteindre **2 % du chiffre d'affaires mondial** de l'entité concernée. En plus des amendes, il existe également un risque de **préjudice à la réputation.**

8. Implications et perspectives

- **Changement culturel :** DORA appelle à un changement culturel, en favorisant de nouvelles compétences, une culture de la résilience et une approche collaborative et orientée vers l'apprentissage en matière de gestion des risques.
- **Alignement stratégique :** DORA encourage une structure de gouvernance intégrée et une vision proactive des risques numériques, nécessitant un alignement entre les opérations commerciales et les systèmes d'information.
- **Adaptation technologique :** DORA promeut l'utilisation d'architectures flexibles et modulaires, de solutions d'automatisation intelligente et de capacités de réponse en temps réel.
- **Calendrier :** DORA doit être appliqué à partir du **17 janvier 2025.**

9. Étapes de transformation : un voyage méthodologique



1

Diagnostic initial

- Évaluation exhaustive des systèmes informatiques existants
- Identification des vulnérabilités et des gaps de résilience opérationnelle
- Cartographie précise des infrastructures technologiques

2

Planification stratégique

- Définition d'une feuille de route claire et progressive
- Alignement des objectifs techniques avec la stratégie globale de l'entreprise
- Priorisation des actions de modernisation et de sécurisation

3

Implémentation technique

- Mise en place de contrôles de résilience avancés
- Déploiement de solutions d'automatisation et d'orchestration
- Renforcement des mécanismes de détection et de réponse aux incidents

Approche progressive : construire la résilience par itérations

L'approche recommandée par les experts en cybersécurité (ENISA, 2023) est celle d'une transformation incrémentale. Cette méthode permet de :

- Minimiser les disruptions opérationnelles
- Permettre des ajustements continus
- Gérer efficacement les ressources et les budgets
- Maintenir un niveau de service constant

Gestion du changement : au-delà de la technique

La transformation DORA dépasse les aspects purement techniques. Elle nécessite une approche holistique de gestion du changement, comme le souligne le rapport McKinsey sur la transformation digitale (2023).

Axes Stratégiques

1. Communication transparente
   - Expliquer les enjeux et les bénéfices de DORA
   - Créer une narratif positif autour de la transformation
2. Alignement organisationnel
   - Impliquer tous les départements
   - Créer des comités transversaux
   - Définir des objectifs communs

Formation et culture organisationnelle : le moteur de la résilience

La réussite de DORA repose fondamentalement sur le facteur humain. Selon les recommandations de l'ISACA (Information Systems Audit and Control Association, 2024), la formation doit être :

- **Comprehensive** : Couvrant tous les niveaux hiérarchiques
- **Continue** : Avec des mises à jour régulières
- **Pratique** : Axée sur des scenarios concrets
- **Adaptative** : Tenant compte de l'évolution des menaces

Parcours de formation recommandé

1. Sensibilisation générale
2. Formation technique approfondie
3. Exercices de simulation de crise
4. Certification spécialisée

10. Points importants supplémentaires

Exemptions : DORA prévoit des exemptions pour certains acteurs, notamment :

- Les fournisseurs tiers de services TIC au sein du Système européen de
- banques centrales.
- Les entités financières fournissant des services TIC à d'autres entités
- financières au sein du même groupe.
- Les fournisseurs tiers de services TIC opérant uniquement dans un État
- membre.

Interopérabilité avec NIS2 : DORA est considéré comme un acte sectoriel spécifique dans le cadre de la directive NIS2*.

NIS2 est la Directive (UE) 2022/2555

Testeurs internes :Les testeurs internes peuvent être utilisés pour les tests de pénétration guidés par des menaces (TLPT), sous réserve d'une approbation de supervision et de l'absence de conflits d'intérêts.

11. Conclusion : DORA - une transformation au-delà de la conformité réglementaire

L'émergence d'un nouveau paradigme opérationnel

Le règlement DORA ne représente pas simplement un ensemble de contraintes réglementaires, mais l'expression d'une mutation profonde des écosystèmes numériques financiers. Nous sommes à l'aube d'une transformation qui transcende les approches traditionnelles de gestion des risques technologiques.

Une vision stratégique globale

L'automatisation et l'orchestration ne sont plus de simples leviers techniques, mais des composantes stratégiques centrales de la résilience organisationnelle. Elles incarnent la capacité des entreprises à :

- Anticiper plutôt que subir
- Transformer les contraintes en opportunités
- Construire une agilité opérationnelle dynamique

Les dimensions transformatrices de DORA

Au-delà de la technique : une révolution culturelle

DORA engage une transformation qui dépasse largement les aspects technologiques :

1. Dimension humaine :
    a. Développement de nouvelles compétences
    b. Culture de la résilience
    c. Approche collaborative et apprenante
2. Dimension stratégique :
    a. Alignement entre métiers et systèmes d'information
    b. Gouvernance intégrée
    c. Vision proactive des risques numériques
3. Dimension technologique :
    a. Architectures modulaires et adaptatives
    b. Solutions intelligentes d'automatisation
    c. Capacités de réponse en temps réel

Les perspectives

Un écosystème numérique en mutation
DORA s'inscrit dans une tendance mondiale de :

- Renforcement de la cybersécurité
- Digitalisation accélérée
- Gestion dynamique des risques

Les enjeux émergents

- Intelligence artificielle et gestion des risques
- Souveraineté numérique
- Éthique et résilience technologique

Un investissement, pas un coût
La conformité DORA doit être perçue comme :

- Un accélérateur de performance
- Un différenciateur concurrentiel
- Un levier de transformation digitale

Recommandation finale

Adopter une approche holistique, agile et stratégique.

Ne pas voir DORA comme une contrainte, mais comme une opportunité unique de :

- Moderniser son système d'information
- Développer une culture de l'innovation
- Renforcer sa résilience opérationnelle

Appel à l'action

Les organisations qui réussiront seront celles qui :

- Anticipent
- Investissent dans leurs équipes
- Cultivent une vision dynamique de la transformation

DORA n'est pas une destination, mais un voyage vers l'excellence opérationnelle.

11. Références et Définitions clés

- Gartner Research Report "IT Asset Management" (2022) souligne que les organisations disposant d'une cartographie précise réduisent leurs risques opérationnels de 40%.
- L'étude McKinsey "Digital Transformation in Financial Services" recommande l'utilisation de plateformes de découverte automatique avec des capacités d'apprentissage machine.
- L'Autorité bancaire européenne (ABE) recommande des systèmes de surveillance avec des capacités d'analyse prédictive.
- L'étude ENISA "Cybersecurity Landscape" (2022) précise que 68% des incidents peuvent être anticipés par des systèmes de monitoring intelligents.
- *Le rapport Deloitte "Cyber Resilience" (2023) indique que l'automatisation des tests réduit les temps de détection des vulnérabilités de 60%*
- *NIST Special Publication 800-53A recommande des approches de tests automatisés et reproductibles*
- *Selon le rapport Gartner "Enterprise Risk Management" (2022), les organisations dotées de solutions avancées de gestion des risques réduisent leurs incidents opérationnels de 45%*
- *McKinsey souligne que ces plateformes deviennent des "centres de décision intelligents"*
- *Le rapport NIST Special Publication 800-53A recommande des approches de tests :*
  - *Reproductibles*
  - *Exhaustifs*
  - *Adaptables*
- *Une étude conjointe MIT-Harvard démontre que l'IA peut réduire les temps de détection des incidents de 70% dans le secteur financier.*
- ***Références complètes :***
  - *Gartner, Enterprise Risk Management Report, 2022*
  - *McKinsey, Digital Transformation in Financial Services, 2022*
  - *Guidelines EBA/GL/2021/04, Autorité bancaire européenne*
  - *NIST Special Publication 800-53A*
  - *MIT-Harvard Joint Study, AI in Financial Risk Management, 2022*
  - *Règlement (UE) 2022/2554 DORA*

12. Définitions clés

- **Fournisseur tiers de services TIC** : Une entreprise fournissant des services TIC.
- **Fournisseur intra-groupe de services TIC :** Une entreprise au sein d'un groupe financier qui fournit principalement des services TIC à d'autres entités du même groupe.
- **Services TIC :** Services numériques et de données fournis via des systèmes TIC, y compris les services matériels en tant que service, à l'exclusion des services téléphoniques analogiques traditionnels.
- **Risque de concentration TIC :** L'exposition à un ou plusieurs fournisseurs tiers critiques de services TIC, individuellement ou collectivement.

13. FAQ

Quel est le champ d'application du Règlement sur la Résilience Opérationnelle Numérique (DORA) ?

DORA s'applique à une large gamme d'entités financières, notamment les institutions de crédit, les établissements de paiement, les fournisseurs de services d'information sur les comptes, les établissements de monnaie électronique, les entreprises d'investissement, les fournisseurs de services liés aux crypto-actifs, les entreprises d'assurance et de réassurance, ainsi que les fournisseurs tiers de services TIC.

Il vise à garantir que l'ensemble de l'écosystème financier, et pas seulement les institutions financières traditionnelles, puisse résister aux perturbations liées aux technologies de l'information et de la communication (TIC).
DORA ne s'applique pas aux gestionnaires de fonds d'investissement alternatifs, aux institutions de retraite professionnelle comptant au total 15 membres ou moins, ni aux institutions de type « giro postal ».

Quelles sont les principales exigences de DORA concernant la gestion des risques TIC pour les entités financières ?

DORA impose une approche proactive pour gérer les risques TIC. Les entités financières doivent:

- Cartographier précisément leurs systèmes TIC,
- Identifier de manière exhaustive les vulnérabilités potentielles,
- Mettre en œuvre des mesures pour prévenir et atténuer les perturbations.

Cela inclut :

- L'établissement d'un cadre robuste de gestion des risques TIC,
- Des tests réguliers de la résilience des systèmes (y compris des tests de pénétration),
- L'élaboration de plans de réponse et de reprise en cas d'incident.

Les entités doivent également développer et maintenir une politique sur l'utilisation des services TIC fournis par des tiers.

Comment DORA affecte-t-il la gestion des fournisseurs tiers de services TIC ?

DORA étend considérablement la responsabilité des entités financières dans la gestion de leurs fournisseurs tiers de services TIC. Cela comprend :

- Une évaluation rigoureuse des fournisseurs TIC,
- L'intégration de clauses contractuelles spécifiques pour protéger leur résilience,
- La gestion des risques liés à la dépendance technologique, y compris la concentration des risques TIC,
- La surveillance des procédures de gestion des vulnérabilités des fournisseurs,
- Le suivi de l'intégrité des données, même dans des environnements non productifs.

FAQ

Qu'est-ce qu'un fournisseur tiers de services TIC "critique" et comment est-il désigné ?

Un fournisseur tiers de services TIC est considéré comme "critique" si sa défaillance pourrait avoir un impact systémique significatif sur la stabilité, la continuité ou la qualité des services financiers.
La désignation repose sur des critères quantitatifs et qualitatifs, notamment :

- Le nombre d'entités financières desservies,
- La valeur totale des actifs de ces entités,
- Leur importance systémique (G-SIIs ou O-SIIs),
- Le degré de substituabilité du fournisseur.
- Les fournisseurs tiers critiques sont soumis à un cadre de supervision.

Quelles sont les exigences pour un registre des informations relatives aux contrats TIC ?

Les entités financières doivent :

- Maintenir et mettre à jour régulièrement un registre détaillé des informations relatives à tous leurs contrats avec des fournisseurs tiers TIC,
- Inclure des données sur le type de services TIC, la localisation des fournisseurs, la nature des données partagées, et des informations sur la chaîne d'approvisionnement TIC.
- Ce registre doit utiliser des modèles standardisés et inclure des points de données spécifiques (dates de début et de fin des contrats, droit applicable, plan de sortie, etc.).

Qu'est-ce que le test de pénétration guidé par les menaces (TLPT) et comment est-il utilisé dans le cadre de DORA

Le TLPT est une évaluation de cybersécurité qui simule une cyberattaque réelle pour évaluer la résilience des systèmes d'une entité financière.
DORA exige que certaines entités financières effectuent des TLPT sur leurs systèmes critiques. Les testeurs internes peuvent être utilisés à condition qu'ils soient indépendants, qu'il n'y ait pas de conflits d'intérêts, et qu'une alternance soit prévue entre testeurs internes et externes. Cependant, l'intelligence sur les menaces utilisée pour le TLPT doit toujours provenir d'un fournisseur externe.

Quels sont les aspects clés des risques TIC résiduels acceptés ?

Les entités financières peuvent accepter des risques TIC résiduels lorsqu'une atténuation complète n'est pas réalisable ou rentable. Cela nécessite :

- Une acceptation formelle par les organes de gouvernance,
- La création d'un inventaire de ces risques, avec justification,
- Une revue annuelle de ces risques, y compris les changements éventuels et les mesures d'atténuation disponibles.

FAQ

Quelles sont les conséquences potentielles d'une non-conformité avec DORA ?

La non-conformité avec DORA peut entraîner :

- Des amendes pouvant atteindre 2 % du chiffre d'affaires mondial,
- Des dommages à la réputation,
- Des répercussions sur la stabilité du système financier,
- Des actions réglementaires ou juridiques supplémentaires.

Smartbot Consulting

Smartbotconsulting.com

contact@smartbotconsulting.com