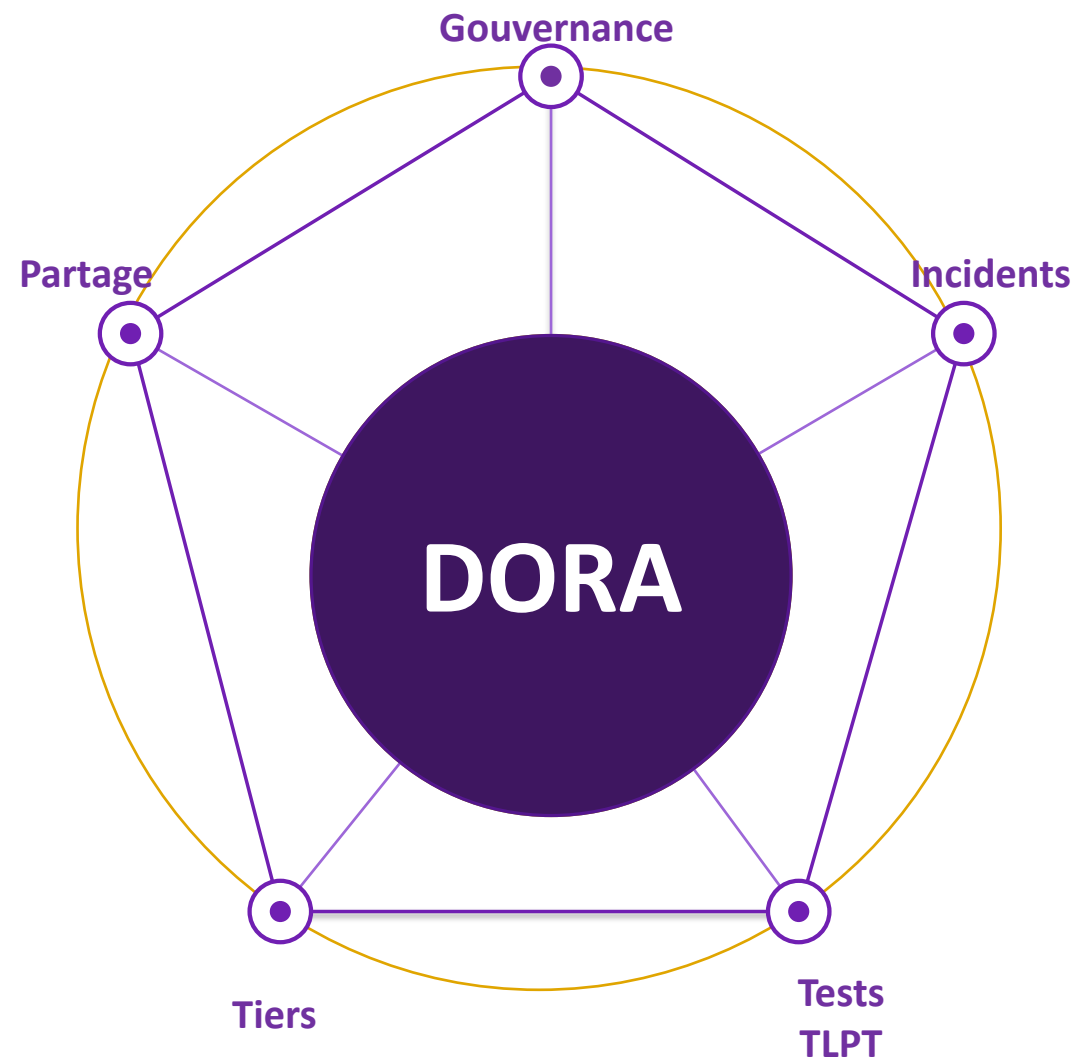


DORA

De la cybersécurité à la résilience systémique

Applicable depuis le 17 janvier 2025

- Entités financières + Prestataires TIC critiques
- 5 piliers : Gouvernance, Incidents, Tests, Tiers, Partage
- Sanctions : jusqu'à 2% du CA, responsabilité CA



Pourquoi DORA ? La fin des architectures en silo

POINT DE RUPTURE

Le risque n'est plus applicatif :

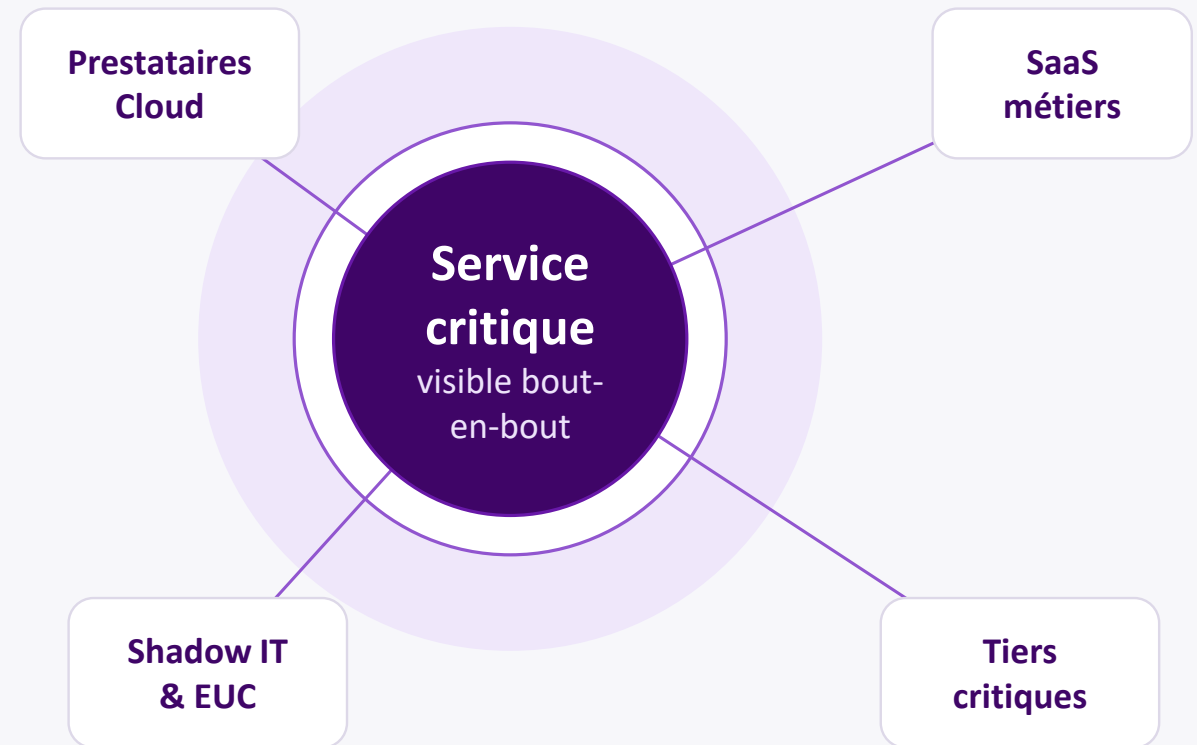
il devient systémique.

DORA oblige à relier

- fournisseur,
- composant,
- application
- et service métier

dans une même lecture de résilience.

Objectif : prouver la continuité des services critiques sous stress.



DORA change la focale : de la conformité documentaire vers la résilience mesurable de la chaîne TIC.

Mise en application : cas concret sur le terrain

TERRAIN

Captive financière

- SI hybride multinationale
- Cloud & Legacy

Pressions réglementaires

BCE / BCBS 239 / DORA

Cible

Relier SI, CMDB et référentiel EA
Analyse d'impact
Conformité BCE

3 chantiers pour rendre le référentiel vivant

01

Convergence CMDB & Référentiel d'AE

Synchronisation API entre CMDB et référentiel EA.
Passage du serveur au service pour cartographier les dépendances réelles.

02

Obsolescence automatisée

Observabilité via Dynatrace et tags dynamiques pour détecter et signaler les composants obsolètes.

03

BIA / PRA — sortir de la “guerre Excel”

220 applications EUC immatriculées.
Plans de reprise structurés en remplacement des tableurs statiques.

Résultat : un référentiel vivant, détectable, aligné sur les services critiques.

Difficultés, angles morts et paradoxes

LE RISQUE CACHÉ

Confondre inventaire et maîtrise.

La conformité se fragilise quand les données, les responsabilités et les arbitrages restent dispersés.

5

Anti-patterns
à surveiller

Angles morts observés sur le terrain

- 1 **Guerre sémantique** — Applications renommées “composants techniques” pour sortir du périmètre.
- 2 **Identifiants fourre-tout** — Plateforme, bases et services regroupés sous un code unique : criticité indiscernable.
- 3 **Quickwin** — Import massif = dette technique invisible si la qualité de donnée n’est pas pilotée.
- 4 **Syndrome Excel** — Registres et droits gérés en fichiers statiques : faible traçabilité.
- 5 **Déficit de sponsoring** — La résilience perçue comme un chantier architecture, pas comme un risque stratégique.

À retenir : la résilience DORA dépend autant des données que de l’architecture.

L'organisation idéale pour DORA

PRINCIPE DIRECTEUR

Piloter par le haut, et opérer en transversal.

DORA n'est pas un chantier d'architecture isolé : c'est un risque stratégique qui exige un sponsor métier fort au COMEX.

2%

du CA mondial :
sanctions possibles
+ responsabilité du CA

Sponsor COMEX actif : arbitrages,
standards et adoption

Modèle opérationnel cible : responsabilités partagées

Task Force transversale — Métiers · IT/DevOps · Sécurité · Conformité

QUI FAIT QUOI ?

01

Métiers

Identifient les FCI et les saisissent dans le référentiel unifié ; fin des Excel morts.

02

Architecture d'Entreprise

Modélise les dépendances, traque le Shadow IT / SSO et démasque les incohérences.

03

IT / DevOps / Production

Maintient une CMDB propre et automatise vulnérabilités & obsolescence via observabilité.

04

Risque, Contrôle & Conformité

Se branche aux données EA pour audits, workflows, RTO/RPO et preuves réglementaires.

Conduite du changement : pédagogie continue, frictions réduites, double saisie supprimée, référentiel vivant.

De la cartographie, au pilotage GRC

LE PASSAGE À L'ÉCHELLE

**L'EA produit la vérité opérationnelle ;
la GRC orchestre l'action.**

L'amélioration : passer d'une logique "inventaire" à une chaîne de pilotage mesurable, alimentée par une donnée d'architecture fiable.

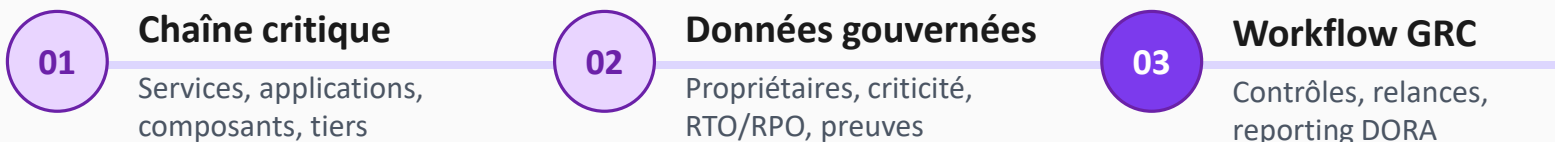


Sans propriétaire, criticité et preuves à jour, la GRC accélère surtout les écarts.

EA fiable → GRC pilotable

PRÉREQUIS

3 leviers de bascule



À retenir : la GRC industrialise le suivi ; l'urbanisation rend la conformité fiable.

Marte vous accompagne
Architecture d'entreprise · GRC · DORA
marTE.fr