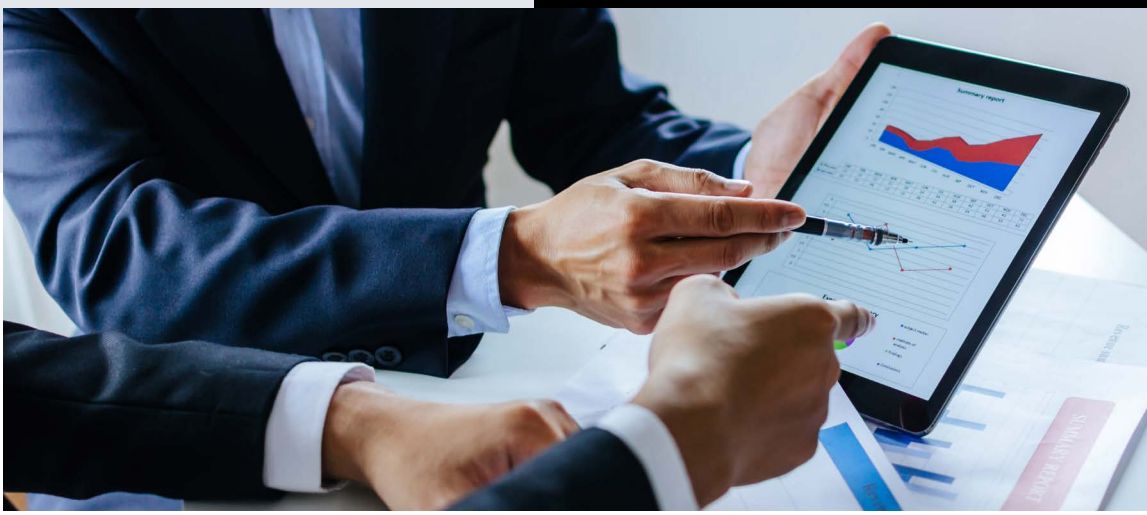
LE DIGITAL OPERATIONAL RESILIENCE ACT

Analyse du règlement DORA

Vers une stratégie de résilience opérationnelle informatique

CGI BUSINESS CONSULTING

01



FICHE D'IDENTITÉ DE DORA (DIGITAL OPERATIONAL RESILIENCE ACT)

Une évolution indispensable de la réglementation bâloise

Depuis la règlementation bâloise de 2005, les établissements **déterminent leurs fonds propres exigibles en considérant également le risque opérationnel**. DORA vient renforcer les lignes directrices de l'EBA (European Banking Authority) du 21 mars 2018 et l'arrêté du 3 novembre 2014 pour compléter un dispositif sur le risque informatique connu et maîtrisé par le secteur financier.

La réglementation requiert des acteurs du secteur financier et assurantiel de compléter l**e cadre de contrôle interne**.

Mise en place d'une stratégie de résilience opérationnelle informatique →

- Gestion des risques IT
- Déclaration des incidents liés aux technologies
- Tests de résilience opérationnelle IT
- Prise en compte du risque sur les tiers

→ Meilleure gestion des incidents

→ Renforcement des actions anti-intrusion

→ Enrichissement des plans de continuité d'activité

DORA impose une implication au plus haut niveau des instances dirigeantes

Objectifs poursuivis

Renforcer la résilience opérationnelle numérique des entités du secteur financier et assurantiel de l'Union européenne en rationalisant les règles en vigueur et en introduisant de nouvelles exigences dans les domaines où il existait des lacunes.

Ce but est structuré en 3 objectifs généraux comprenant 8 sous-objectifs spécifiques :

1. Réduire le risque de perturbation et d'instabilité financière

- Parer aux risques informatiques de manière plus intégrée et renforcer le niveau global de résilience numérique du secteur
- Veiller à ce que les entités financières évaluent l'efficacité de leurs mesures de prévention et de résilience et détectent les vulnérabilités
- Renforcer les garanties contractuelles avec les tiers fournisseurs services informatiques, y compris en ce qui concerne les règles d'externalisation

2. Réduire la charge administrative et accroître l'efficacité de la surveillance

- Rationaliser les notifications d'incidents et résoudre les problèmes de chevauchement des exigences en matière de notification
- Réduire la fragmentation du marché unique et favoriser la reconnaissance transfrontière des résultats des tests
- Permettre une supervision des activités des tiers prestataires critiques de services informatiques

3. Renforcer la protection des consommateurs et des investisseurs

- Permettre aux autorités de surveillance financière d'avoir accès aux informations sur les incidents
- Encourager l'échange de renseignements sur les menaces dans le secteur financier

Acteurs et pays concernés

Banque et finance

- Etablissements de crédit
- Etablissements de paiement
- Etablissements de monnaie électronique
- Entreprises d'investissement
- Sociétés de gestion
- Gestionnaires de fonds d'investissement alternatifs
- Contreparties centrales
- Plateformes de négociation
- Dépositaires centraux de titres
- Prestataires de communication de données
- Administrateurs d'indices de référence d'importance critique
- Agences de notation de crédit
- Référentiels centraux
- Référentiels des titrisations

Finance alternative

- Prestataires sur crypto-actifs, émetteurs de crypto-actifs, émetteurs de jetons
- Prestataires de financement participatif

Assurance

- Entreprises d'assurance, de réassurance, intermédiaires d'assurance et de réassurances, intermédiaires d'assurance à titre accessoire
- Institutions de retraite professionnelle

Autre

- Contrôle légaux des comptes
- Cabinets d'audit
- Tiers prestataires de services informatiques

Il s'agit d'un règlement européen qui s'applique **aux entités financières et assurantielles** règlementées **au niveau de l'Union.**

Les **filiales européennes règlementées en Europe de grands groupes étrangers** se voient appliquer DORA.

Les dates clés

Processus législatif

Consultation publique

Période de contribution 19 décembre 2019 – 16 janvier 2020.

Discussions entre les Co-législateurs de l'Union

25 janvier 2022 : début du trilogue entre les co-législateurs de l'Union.

11 mai 2022 : le Conseil et le Parlement européen sont parvenus à un accord politique provisoire.

Entrée en application de DORA

Entrée en application de DORA :

- **Entrée en vigueur : 16 janvier 2023**, soit 20 jours après la publication au JOUE du 27/12/2022
- **Entrée en application : 17 janvier 2025**
- Le règlement **sera ensuite d'application immédiate et intégré à la législation de chaque État membre** de l'UE
- **Première phase de contrôle à prévoir par l'ACPR ou l'AMF** : dès l'entrée en application, bien qu'une période de tolérance puisse être prévue

5 thématiques issues du texte

1.

Gestion des risques informatiques (art. 4 à 14)

Objectifs : S'assurer du bon fonctionnement et de la mise à jour des mesures de contrôles

2.

Gestion, classification et notification des incidents liés à l'informatique (art. 15 à 20)

Objectifs : Harmoniser et centraliser les notifications des incidents à des fins de transmission aux autorités

3.

Test de Résilience opérationnelle numérique (art. 21 à 24)

Objectifs : Tester l'efficacité des dispositifs de gestion des risques et des mesures en place afin de limiter les effets sur les activités critiques et importantes

4.

Gestion des risques liés aux tiers prestataires de services informatiques (art. 25 à 39)

Objectifs : Vérifier le niveau de contrôles suffisants de leurs tiers, tout particulièrement les PCI (Prestations Critiques ou Importantes) et mettre en place les mesures de surveillance requises

5.

Partage d'informations et de renseignements (art. 40)

Objectifs : Mettre en place des accords de partage d'informations entre entreprises pour faire face au cybermenaces, et communiquer avec l'autorité de régulation

Certaines thématiques sont déjà traitées, a minima partiellement, par des acteurs internes ou dans des référentiels connus.

Il faut donc identifier les acteurs internes et s'appuyer sur l'état de l'art interne & externe pour ne pas dupliquer les efforts.

02

RESPONSABILITÉS ET SANCTIONS

Sanctions prévues

Types de sanction			
Matérielles	Financières et économiques	Réputationnelles	Pénales

Elles sont laissées à la discrétion des Etats-Membres (art. 46)

GOUVERNANCE

Définir les rôles et responsabilités pour les fonctions liées à l'informatique.

Mettre en place les moyens d'être informé des incidents liés à l'informatique et de leurs conséquences

SUIVI DE LA GESTION DES RISQUES INFORMATIQUES

Déterminer le niveau approprié de tolérance au risque.

Gérer l'ensemble des processus d'approbation et de contrôle des risques informatiques (politique de continuité d'activité, plan de rétablissement après sinistre informatique, plans d'audits).

Organe de direction
Principe général de pleine responsabilité

POLITIQUE CONCERNANT L'UTILISATION DE SERVICE INFORMATIQUES FOURNIS PAR DES TIERS

Approuver les modalités d'utilisation des services informatiques fournis par des tiers.

Etre informé des accords conclus avec ces tiers sur l'utilisation des services (changements éventuels, analyses de risques associés).

GESTION DU BUDGET

Allouer le budget approprié à la résilience opérationnelle numérique et aux formations sur les risques informatiques.

→ En cas de non respect des obligations : sanctions pénales possibles des organes de direction

03

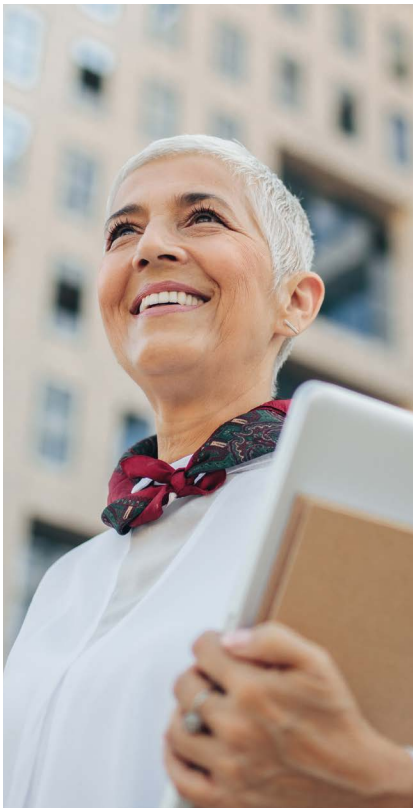
DÉMARCHE ET OFFRE CGI BUSINESS CONSULTING

Vue générale de la démarche

1. COLLECTER → Diagnostic flash / état des lieux de l'existant

2. ANALYSER → Analyse d'écart DORA

3. AMELIORER → Feuille de route DORA



Par le biais de l'outil de diagnostic CGI DORA

Gestion des risques informatiques	Gestion des incidents et tests de résilience	Gestion des risques liés aux tiers
COLLECTER		
Identifier l'existant : **gouvernance, politiques, procédures, stratégies, analyse de risque**	Identifier l'existant : **détection, suivi, notification des incidents, politique de continuité des activités informatiques, programme de test, réalisation de tests**	Identifier l'existant : **registre des services et des fonctions** fournis par les tiers, **suivi contractuel, suivi des risques liés à l'externalisation, moyens de contrôle et de mitigation de ces risques**
ANALYSER		
Identifier les écarts avec les exigences de DORA (à propos des **procédures, politiques, stratégies, gouvernance, système de gestion de la sécurité de l'information** fondé sur des normes internationales reconnues, **évaluation des risques, suivi et contrôle des systèmes** en place, **politique de sauvegarde**)	Identifier les écarts avec les exigences de DORA (à propos des **mécanismes de détection des incidents, processus de gestion des incidents, registre des activités concernées, contrôle après incident, identification et communication des changements de la politique de continuité d'activité, classification des incidents et impacts, programmes de test)**	Identifier les **moyens de contrôle et de mitigation des risques associés à ces prestataires** (à propos du registre des services et des fonctions fournis par les tiers, suivi contractuel, identification des risques liés à l'externalisation, politique relative à l'utilisation des services informatiques fournis par des tiers prestataires de services informatiques, inventaire avec les fonctions opérationnelles liées à l'informatique, les actifs et les configurations et interconnexions liées)
AMELIORER		
1. Répartir les actions identifiées par chantier	2. Formaliser une feuille de route globale Y intégrer les actions réparties par chantier et les rôles et responsabilité des acteurs clés	3. Aider à la mise en place d'une gouvernance Fixer les jalons / les deadlines Fixer les porteurs de chaque action identifiée

CGI BUSINESS CONSULTING

Vous avez des questions sur ce sujet ? N'hésitez pas à nous contacter

Hervé Ysnel

Vice-Président Senior
en charge des activités
conseil sécurité, risque &
continuité d'activité

herve.ysnel@cgi.com

Chez CGI Business Consulting, cabinet de conseil majeur en France, nous sommes audacieux par nature. Grâce à son intimité sectorielle et à sa capacité à mobiliser des expertises diverses, CGI Business Consulting apporte aux entreprises et aux organisations des solutions de conseil audacieuses et sur mesure, pour une réussite stratégique et opérationnelle de leurs projets de transformation.
Nos 1 000 consultants accompagnent nos clients dans la conduite et la mise en œuvre de leurs projets de transformation, dans une relation franche et de confiance, pour leur permettre de prendre les bonnes décisions.
Fondée en 1976, CGI figure parmi les plus importantes entreprises de services-conseils en technologie de l'information (TI) et en management au monde. Elle aide ses clients à atteindre leurs objectifs, notamment à devenir des organisations numériques axées sur le client.

cgi.fr/conseil

L'audace par nature