MAET CONSULTING

CYCOM Risk

Pocket Result

Réglementation DORA

Comment vous préparer d'ici 2025 ?

Livre blanc, Mai 2023

www.maet-consulting.com

MAET CONSULTING

CYCOM Risk

Pocket Result

Sommaire

MAET CONSULTING

CYCOM Risk

Pocket Result

1| Qu'est-ce que la réglementation DORA ?

Le règlement DORA (Digital Operational Resilience Act) a été proposé par la Commission Européenne, en septembre 2020. Le texte a été adopté le 16 janvier 2023, et entrera pleinement en application le 17 janvier 2025.

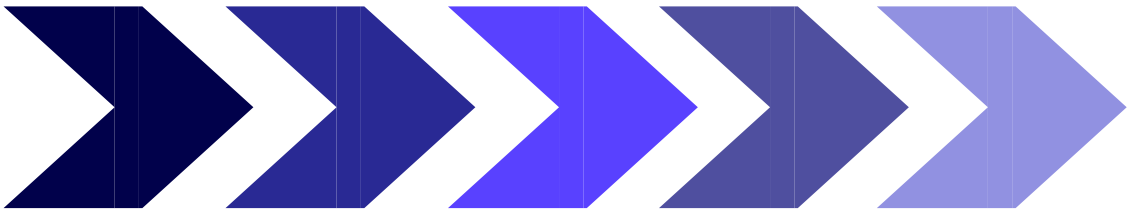
DORA propose un cadre réglementaire pour la gestion des risques liés aux TIC (Technologies de l'Information et de la Communication), visant à renforcer la résilience opérationnelle numérique du secteur financier de l'UE (Union Européenne).

Ainsi, des mesures doivent être mises en place pour les organisations du secteur financier afin :

- de prévenir les incidents de cybersécurité et y répondre ;
- d'assurer leur continuité opérationnelle en cas d'incident ;
- d'améliorer la gestion des risques cyber dans leur ensemble.

16 janv. 2023 Entrée en vigueur du règlement DORA

17 janv. 2025 Entrée en application du règlement DORA



48%

des entreprises ont rapporté des cyberattaques en 2021 (source : Hiscox, 2021).

13M€

Coût moyen d'une cyberattaque pour une grande entreprise (source : Accenture, 2019).

25%

des attaques concernent le secteur financier (source : IBM, 2023).

2| Quels sont ses 5 piliers ?

1. METTRE EN PLACE UN DISPOSITIF DE GESTION DES RISQUES LIÉS AUX TIC

complet et bien documenté, afin de maîtriser ses risques efficacement et d'assurer un niveau élevé de résilience opérationnelle numérique.

Ce dispositif de gestion des risques fait partie intégrante du dispositif global, et doit être mis à jour et amélioré en continu selon les enseignements tirés.

2. FAIRE LE REPORTING DES INCIDENTS TIC ET DES CYBER MENACES

en définissant et en mettant en place un processus de gestion des incidents, afin de les détecter, les gérer et les notifier aux autorités.

Les entités financières doivent ainsi enregistrer et classer les incidents TIC et les cyber menaces selon les critères déterminés par le règlement européen DORA et les autorités européennes de surveillance (AES : EBA, EIOPA et ESMA).

2| Quels sont ses 5 piliers ?

3. ÉTABLIR UN PROGRAMME DE TESTS DE RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE

intégré au dispositif global, maintenu et réexaminé régulièrement par les entités financières (autres que les micro entreprises).

Ce programme de tests doit répondre à certaines conditions :

- Comprendre plusieurs évaluations, tests, méthodologies, pratiques et outils à appliquer ;
- Couvrir l'ensemble des outils et des systèmes TIC ;
- Être réalisé par des parties indépendantes externes ou internes ;
- Prévoir des procédures et des stratégies afin d'assurer la hiérarchisation, la classification et la résolution des problèmes mis en lumière durant les tests ;
- Définir des procédures de revue et de validation de la mise en oeuvre des plans de remédiation.

2| Quels sont ses 5 piliers ?

4. GÉRER LES RISQUES LIÉS AUX PRESTATAIRES DE SERVICES TIC

- Mettre en place un dispositif de maîtrise des risques liés aux tiers prestataires de services informatiques ;
- Définir une politique d'utilisation des services TIC liées aux fonctions jugées critiques ou importantes ;
- Créer et mettre à jour un registre d'informations relatif aux contrats conclus avec les prestataires de services TIC ;
- Conduire des diligences avant tout premier contact, et notamment évaluer le risque de concentration ;
- Intégrer aux contrats des clauses standard minimales, en particulier en matière de résiliation ;
- Surveiller continuellement la relation avec les prestataires de services TIC.

5. INFORMER ET RENSEIGNER D'AUTRES ENTITÉS FINANCIÈRES DE CONFIANCE

au sujet des cyber menaces et cyberattaques observées, dans un souci de sensibilisation et de soutien des capacités de défense, des techniques de détection des menaces ainsi que des stratégies d'atténuation, de réponse et de rétablissement du secteur financier.

MAET CONSULTING

CYCOM Risk

Pocket Result

3| Comment vous préparer d'ici 2025 ?

SENSIBILISATION

Une culture organisationnelle nourrie
par la formation et la sensibilisation des employés,
favorise la résilience opérationnelle,
et par conséquent, la préparation de l'entreprise
face à l'adversité.

ACCOMPAGNEMENT

DORA est l'opportunité de renforcer votre résilience opérationnelle, garantir la protection des données et créer un climat de confiance élevé auprès de toutes vos parties prenantes.
Cela assure votre pérennité et compétitivité dans un monde en constante mutation.

OUTIL

Un outil de pilotage est nécessaire pour assurer et optimiser la mise en conformité de votre organisation avec la réglementation DORA : intégration, pilotage et suivi en temps réel de vos données et de votre dispositif de maîtrise des risques liés aux TIC.

MAET CONSULTING

CYCOM Risk

Pocket Result

SENSIBILISATION

Développez une culture de la résilience opérationnelle numérique.

SENSIBILISEZ & FORMEZ

Sensibilisez et formez vos équipes sur cette réglementation essentielle pour le secteur financier.

MESUREZ LE RISQUE NUMÉRIQUE

Prenez la mesure du risque numérique et bâtissez votre socle de sécurité.

RÉDUISEZ LES RISQUES

Appréhendez et réduisez les risques opérationnels et juridiques.

DÉVELOPPEZ UNE CULTURE DE LA CYBERSÉCURITÉ

Valorisez et développez une culture de la cybersécurité dans votre entreprise.

MAET CONSULTING

CYCOM Risk

Pocket Result

SENSIBILISATION

Déployez des solutions innovantes et collaboratives.

UNE APPROCHE GLOBALE DES RISQUES

Un programme robuste de conformité et de lutte contre la criminalité financière passe par la mise en œuvre de contrôles internes relatifs à la cybersécurité.

La formation et la sensibilisation aux enjeux de cybersécurité permettra de relever les connaissances minimales des collaborateurs et de renforcer l'environnement de contrôle global de l'entreprise.

INNOVATION & TECHNOLOGIE

Par l'intermédiaire de la technologie utilisée, basée sur l'intelligence artificielle, les formations MAET sont disponibles dans différentes langues, et peuvent être adaptées à vos besoins spécifiques et à votre secteur d'activité.

Aussi, les formations MAET sont dispensées par des avatars ultra réalistes, ce qui rend le suivi des modules et les apprentissages plus plaisants et fluides, augmentant ainsi le taux d'engagement des participants.

MÉTHODE HYBRIDE

Grâce au module communautaire (Campus MAET), les apprenants échangent entre eux et avec leur instructeur, de manière fluide et régulière, sur les problématiques en lien avec leur formation.

MAET CONSULTING

CYCOM Risk

Pocket Result

ACCOMPAGNEMENT

Bénéficiez d'une expertise sur-mesure
pour votre mise en conformité.

MOBILISEZ VOTRE ENTREPRISE

Mobilisez votre entreprise autour des changements requis par le règlement DORA, afin de les mettre en œuvre de manière efficace et opportune.

ORGANISEZ VOTRE STRATÉGIE DE DÉFENSE

Anticipez les menaces et protégez vos systèmes d'information.

TIREZ-EN UNE OPPORTUNITÉ

Construisez et créez votre avantage concurrentiel, en transformant cette réglementation en une opportunité commerciale, sécurisant vos relations avec vos clients et fournisseurs.

ÉLABOREZ UN PLAN D'ACTION

Elaborez un plan d'action et priorisez les tâches pour assurer votre conformité à la règlementation.

MAET CONSULTING

CYCOM Risk

Pocket Result

LOGICIEL SAAS

Pilotez et suivez en temps réel
votre dispositif de maîtrise des risques.

COLLECTEZ & ANALYSEZ

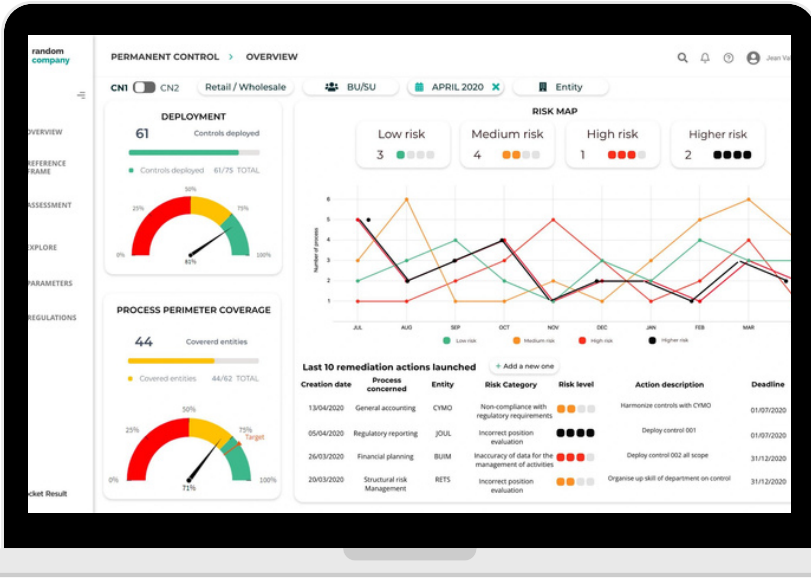
Collectez et analysez des données relatives aux incidents et menaces identifiés.

INTÉGREZ DES PROCESSUS

Intégrez des processus et des données d'externalisation des TIC.

ASSOCIEZ DES MESURES PRÉVENTIVES

Associez au dispositif de maîtrise des risques des mesures préventives et des bonnes pratiques.



MAET CONSULTING

CYCOM Risk

Pocket Result

LOGICIEL SAAS

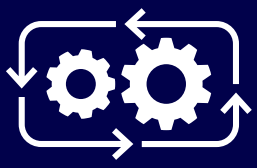
Collaborez facilement grâce à un outil intuitif.
Gagnez du temps dans votre mise en conformité.

COLLABOREZ EN TEMPS RÉEL

Collaborez en temps réel grâce à un outil intuitif, collaboratif, et accessible à tous les métiers.

PARTAGEZ VOS INFORMATIONS

Créez un cadre harmonisé et favorable au partage d'informations.



SUIVEZ EN TEMPS RÉEL

Suivez en temps réel l'exécution des tests et plans de contrôle.

ANTICIPEZ LES RÉGLEMENTATIONS

Évoluez au rythme des réglementations en cours et à venir.

4| Quelques liens utiles

- "Finance numérique : le Conseil adopte le règlement sur la résilience opérationnelle numérique du secteur financier", Communiqué de presse (28/11/2022), Conseil européen / Conseil de l'Union Européenne. Disponible ici.
- The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554. Disponible ici.
- "Le projet de règlement DORA (Digital Operational Resilience Act)", 20/04/2022, Livia Chartrain, juriste, MonJuridiqueInfogreffe. Disponible ici.

5| Contact

Gilles Chevillon
Fondateur & CEO de MAET Consulting

gilles.chevillon@maet-consulting.com
+33 6 26 79 42 91
Gilles Chevillon
https://maet-consulting.com

Frédéric Caubert
Dirigeant de CycomRisk

frederic.caubert@cycomrisk.fr
+33 7 77 31 18 35
Frederic Caubert
https://cycomrisk.fr

Rémy Bellavoine
CEO de Pocket Result

remy.bellavoine@pocketresult.com
+33 6 51 37 91 22
Rémy Bellavoine
https://pocketresult.com

Barbara Carresse
Responsable Marketing chez Pocket Result

bcarresse@pocketresult.com
Barbara Carresse
https://pocketresult.com

Christophe Bardy
Co-fondateur de GRACES Community

christophe@graces.community
+33 6 64 33 19 07
Christophe Bardy
https://www.graces.community