MAET CONSULTING

NIS2 DIRECTIVE

Directive NIS2
Comment préparer votre mise en conformité

Livre blanc, Août 2024

www.maet-consulting.com

MAET CONSULTING

NIS2 DIRECTIVE

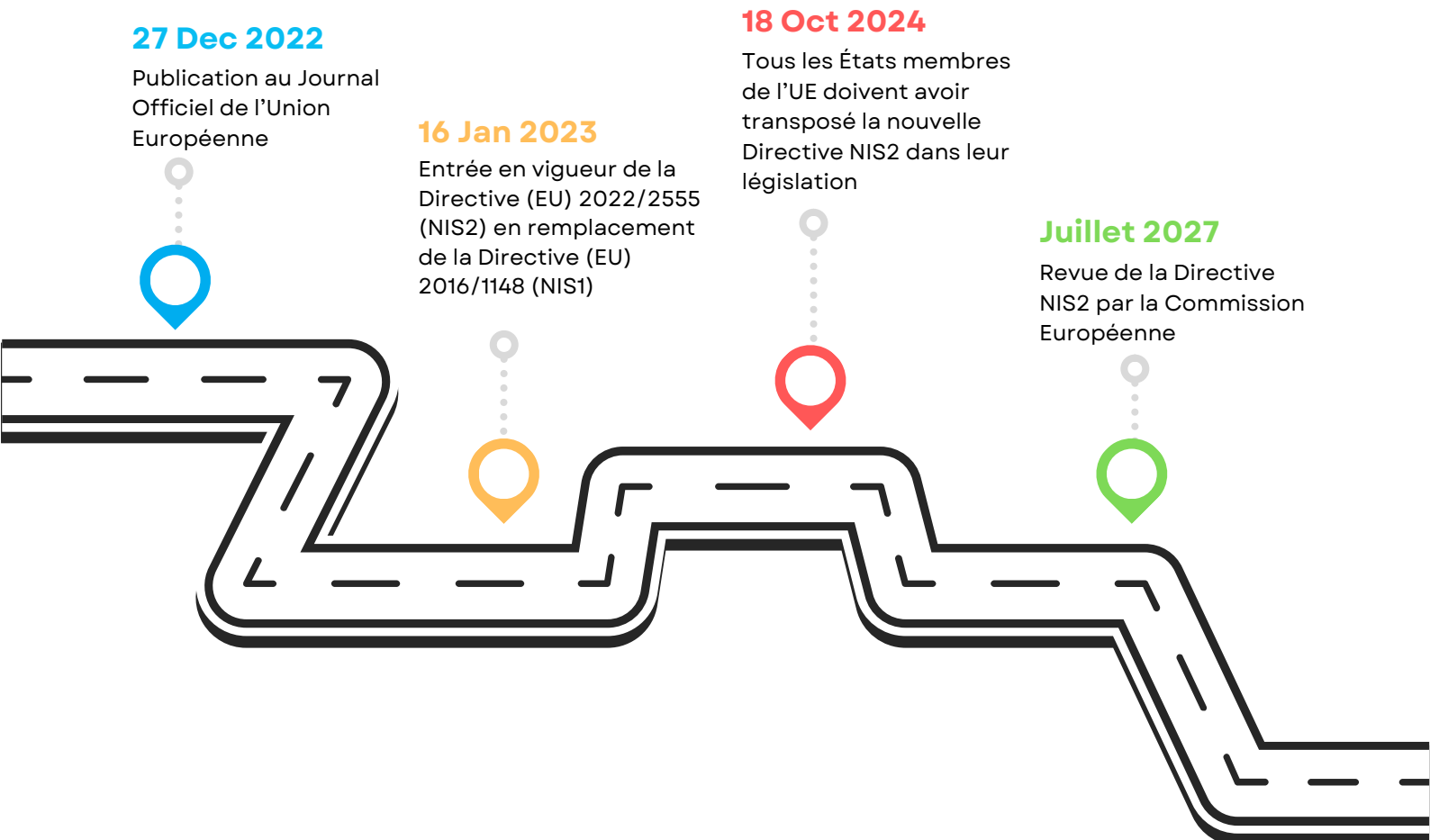
Sommaire

1| Qu'est-ce que la Directive NIS2 ?

Face à la transformation numérique rapide et l'exposition à de nouvelles cybermenaces, le parlement Européen et l'Union Européenne ont adopté en juillet 2016 la directive NIS : Network and Information Security.

Transposée dans le droit français en 2018, la directive avait pour objectif d'atteindre un niveau commun élevé de sécurité des réseaux et des systèmes d'informations dans toute l'UE. Pour cela, les Opérateurs de Services Essentiels (OSE) disposaient de 3 ans pour appliquer 23 règles de sécurité.

Néanmoins, en 2023, le constat est le suivant : les cyberattaques sont de plus en plus perfectionnées et la menace évolue plus rapidement que le niveau de sécurité des secteurs concernés. Face à des acteurs malveillants toujours plus performants et mieux outillés, touchant de plus en plus d'entités trop souvent mal protégées, la directive NIS 2 élargit ses objectifs et son périmètre d'application pour apporter davantage de protection.



2| Les objectifs de la Directive NIS2

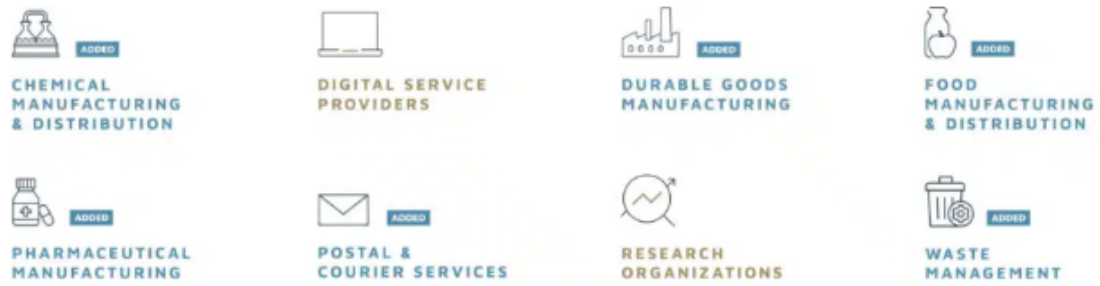
La Directive NIS2 de l'Union européenne impose de nouvelles exigences aux entreprises, les obligeant à renforcer leur cybersécurité, à réaliser des audits réguliers et à signaler rapidement les incidents.

La conformité est obligatoire pour les organisations fournissant des services essentiels, mais elle est également indispensable pour celles souhaitant devenir leurs fournisseurs.

3| Qui est concerné par la Directive NIS2 ?

Secteurs Essentiels

Secteurs Importants



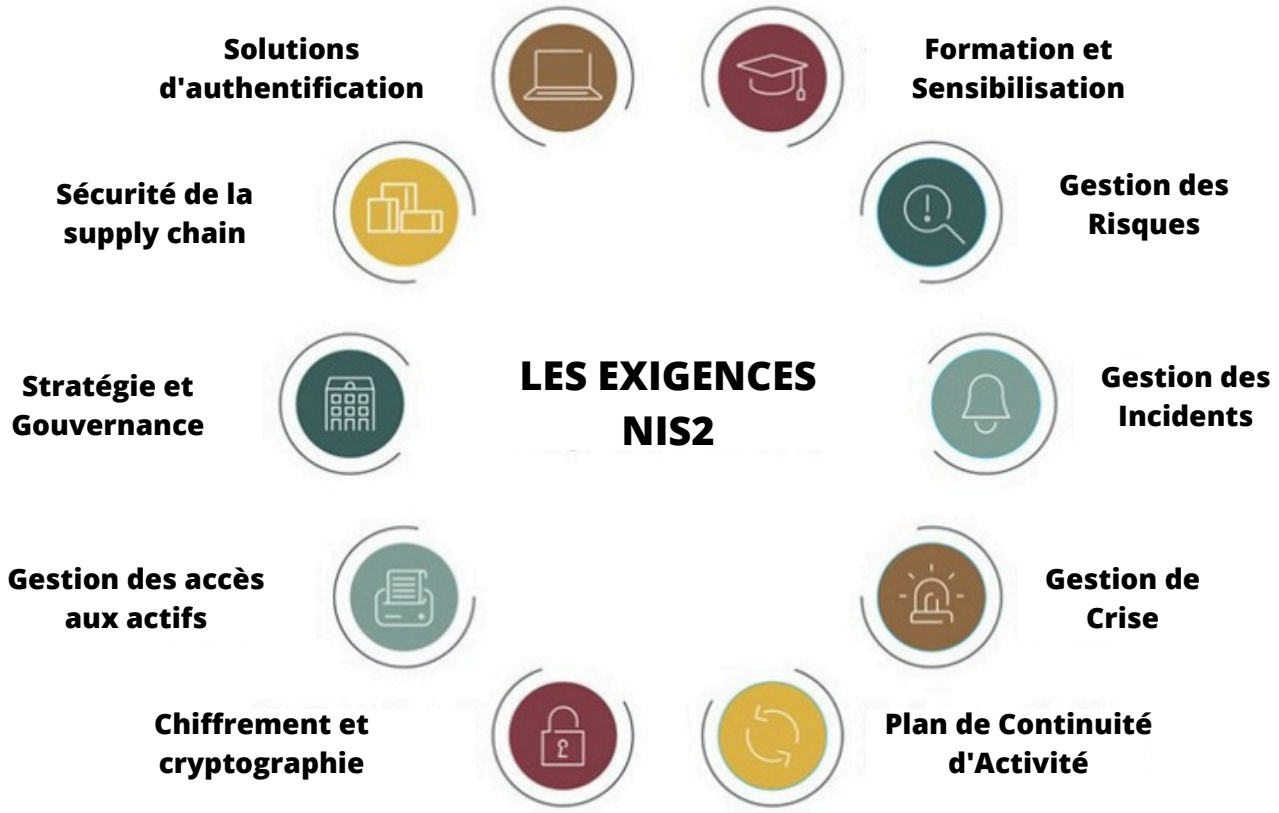
Seuils

TAILLE ENTITE	NOMBRE D'EMPLOYÉS	CHIFFRE D'AFFAIRES (MILLIONS D'EUROS)	BILAN ANNUEL (MILLIONS D'EUROS)	TYPE D'ENTITE
INTERMÉDIAIRE ET GRANDE	x ≥ 250	y ≥ 50	z ≥ 43	ENTITES ESSENTIELLES
MOYENNE	50 ≥ x ≥ 250	10 ≥ y > 50	10 ≥ z > 43	ENTITES IMPORTANTES
MICRO ET PETITE	x < 50	y < 10	z < 10	*Non concernées*

4| Les exigences de la Directive NIS2

La Directive NIS 2 impose aux États membres de mettre en place une stratégie nationale afin d'atteindre et de maintenir un haut niveau de sécurité dans les secteurs susmentionnés.

Les États membres doivent notamment s'assurer que les entités concernées mettent en œuvre les mesures assurant la sécurité de leurs réseaux et systèmes d'information, ainsi que leur environnement physique, selon une approche par les risques appliquée à la cybersécurité.

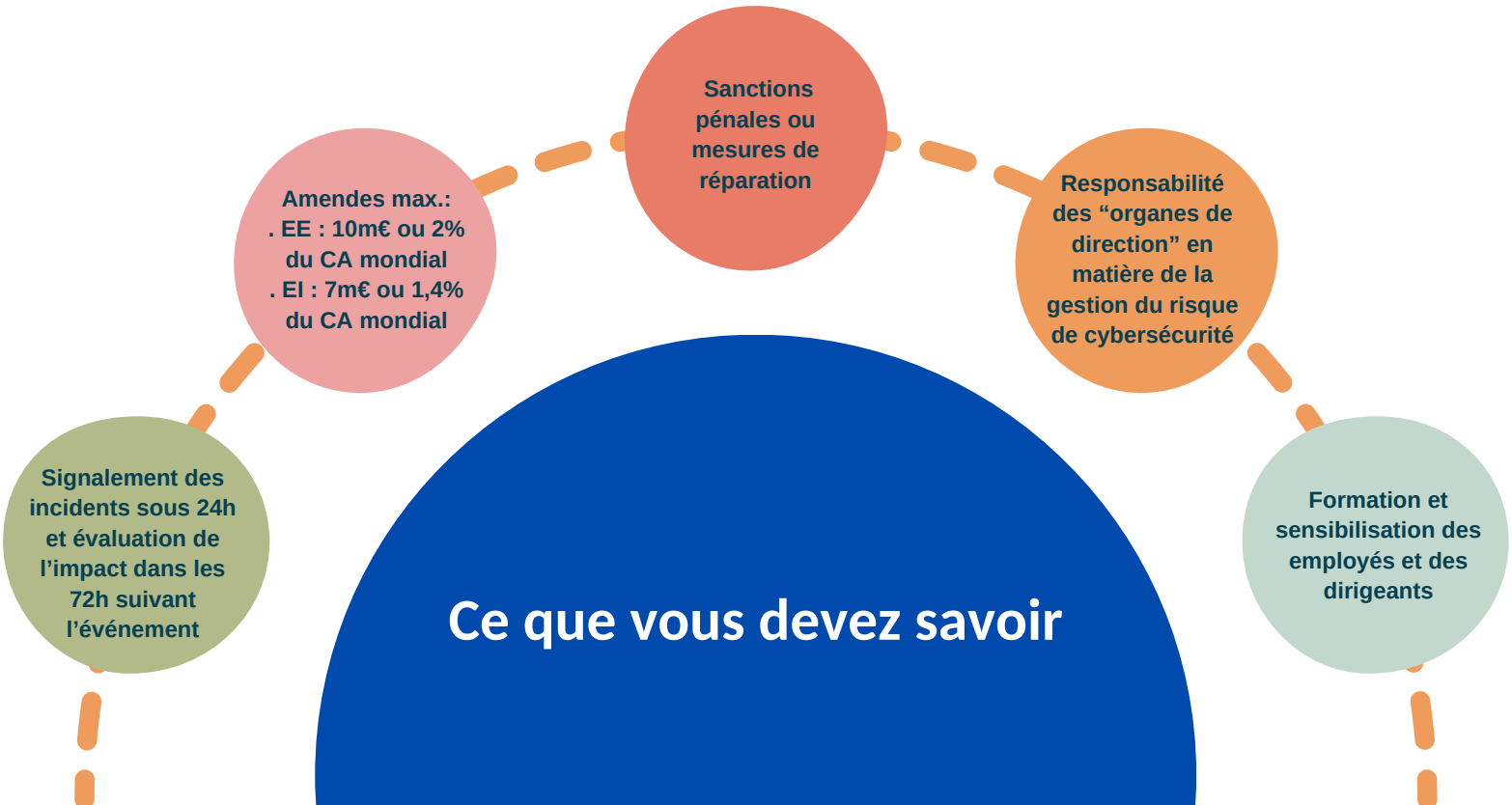


5| Quelles sont les implications de la Directive NIS2 pour votre entreprise ?

Les entreprises concernées sont tenues de respecter les obligations de la Directive NIS2, faute de quoi elles s'exposent à de lourdes sanctions. Ces mesures comprennent des amendes importantes, la révocation de la certification d'une entreprise et la responsabilité personnelle des membres des conseils d'administration.

Le règlement de l'UE attend des conseils d'administration des entreprises qu'ils jouent un rôle actif. Les dirigeants doivent comprendre les nouvelles obligations en matière de gestion des risques et la manière de mettre en œuvre la conformité en matière de sécurité.

Le non-respect des exigences peut entraîner une succession de conséquences graves.



6| Quels sont ses principaux piliers ?

La NIS2 subdivise les secteurs en plusieurs catégories : les entités essentielles et les entités importantes. Si cette catégorisation ne change pas les points sur lesquels vous devez vous aligner pour vous conformer à la NIS2, il existe néanmoins des domaines sur lesquels vous devez porter une attention particulière, en fonction de la catégorie à laquelle vous appartenez.

NIS2 se compose de 46 articles, reposant sur cinq piliers.

1. EXIGENCES EN MATIÈRE DE SÉCURITÉ

La Directive NIS2 impose des mesures techniques et organisationnelles strictes pour protéger les réseaux et les systèmes d'information des opérateurs de services essentiels et des fournisseurs de services numériques.

Cela inclut l'utilisation de pare-feu, de systèmes de détection d'intrusion, de cryptage des données, et la formation continue du personnel en cybersécurité.

Les entreprises doivent effectuer des évaluations régulières des risques et adopter des politiques de sécurité robustes pour prévenir et répondre aux menaces.

2. TRAITEMENT DES INCIDENTS

La gestion des incidents de sécurité est cruciale. Les entités doivent établir des procédures pour détecter, signaler et atténuer rapidement les incidents de sécurité, incluant la surveillance continue et la création de plans d'intervention.

Elles doivent notifier les autorités en cas de violation significative pour minimiser l'impact et rétablir les services rapidement, tout en communiquant avec les parties prenantes.

3. CONTINUITÉ DE SERVICE

Assurer la continuité de service est essentiel pour maintenir la disponibilité des services critiques.

La Directive NIS2 exige que les entreprises élaborent des plans de continuité et de reprise après sinistre, incluant la sauvegarde des données et la redondance des infrastructures.

Elles doivent effectuer des tests réguliers pour vérifier l'efficacité de ces plans et ajuster leurs stratégies en conséquence.

4. SURVEILLANCE, AUDIT ET TESTS

La surveillance proactive, l'audit et les tests réguliers sont essentiels pour assurer la sécurité continue des systèmes.

Les entreprises doivent mettre en place des mécanismes de surveillance pour détecter les anomalies, réaliser des audits de sécurité pour évaluer leur conformité, et effectuer des tests de pénétration et des simulations pour améliorer leur résilience.

5. CONFORMITÉ AUX NORMES INTERNATIONALES

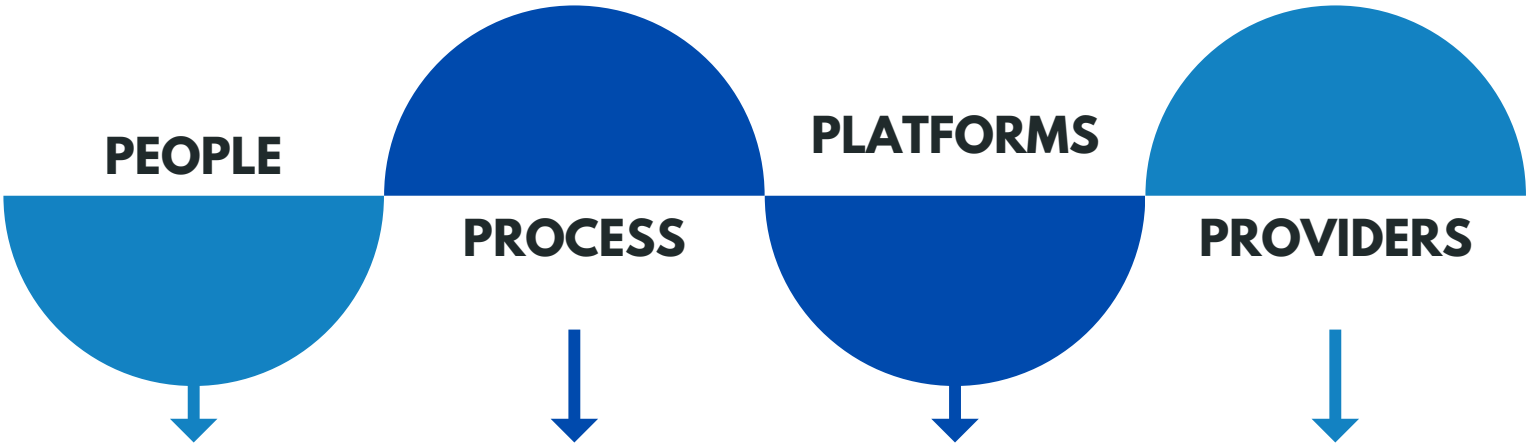
La Directive NIS2 encourage l'adoption de normes internationales de sécurité, telles que l'ISO/IEC 27001, pour assurer une protection harmonisée au sein de l'UE.

La conformité à ces normes aide les organisations à répondre aux exigences légales, améliorer leur sécurité globale et renforcer la confiance des partenaires et des clients.

7| Comment préparer votre mise en conformité

Forts de notre expérience, nous vous recommandons les étapes suivantes :

- Évaluer si la directive NIS2 s'appliquera à votre cas.
- Identifier les manquements par rapport aux exigences de la directive.
- Déterminer les mesures à prendre pour respecter les obligations de gestion.
- Définir un cadre de cybersécurité solide, englobant des mesures à la fois organisationnelles et techniques.
- Mettre en place ces mesures à la fois du point de vue organisationnel et technique au sein de votre organisation.
- Concevoir et implémenter des mécanismes de surveillance pour vérifier l'efficacité de ces mesures en continu.



PEOPLE	PROCESS	PLATFORMS	PROVIDERS
INFORMER, FORMER ET SENSIBILISER CHACUN, DU DÉCIDEUR AU COLLABORATEUR	RENFORCER VOTRE GOUVERNANCE	INVESTIR DANS DES OUTILS ET DES TECHNOLOGIES ADAPTÉS	REVOIR L'ENSEMBLE DE VOS FOURNISSEURS CRITIQUES
• Offre de sensibilisation et de formation complète, modulable et innovante • **En présentiel ou à distance (modules Digital Learning)**	• Conseil et accompagnement (gouvernance, risques, contrôle) • **Support à la mise en conformité** • **Expertise règlementaire et juridique**	• **Tests d'intrusion – Pentest** • **Solution SaaS pour l'analyse de données** • **Définition des KPIs** • **Reporting réglementaire**	• **Identification et classification des fonctions et fournisseurs critiques**

7| Comment préparer votre mise en conformité

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

NIS2 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.

OUTILS

Un outil de pilotage est nécessaire pour assurer et optimiser la mise en conformité de votre organisation avec la Directive NIS2 : intégration, pilotage et suivi en temps réel de vos données et de votre dispositif de maîtrise des risques liés aux tiers.

MAET
CONSULTING

SENSIBILISATION

Développez une culture de la résilience opérationnelle numérique.

SENSIBILISEZ & FORMEZ

Sensibilisez et formez vos équipes sur cette réglementation essentielle pour les secteurs critiques.

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

ACCOMPAGNEMENT

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

MOBILISEZ VOTRE ENTREPRISE

Mobilisez votre entreprise autour des changements requis par la Directive NIS2, 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.

OUTILS

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

COLLECTEZ & ANALYSEZ

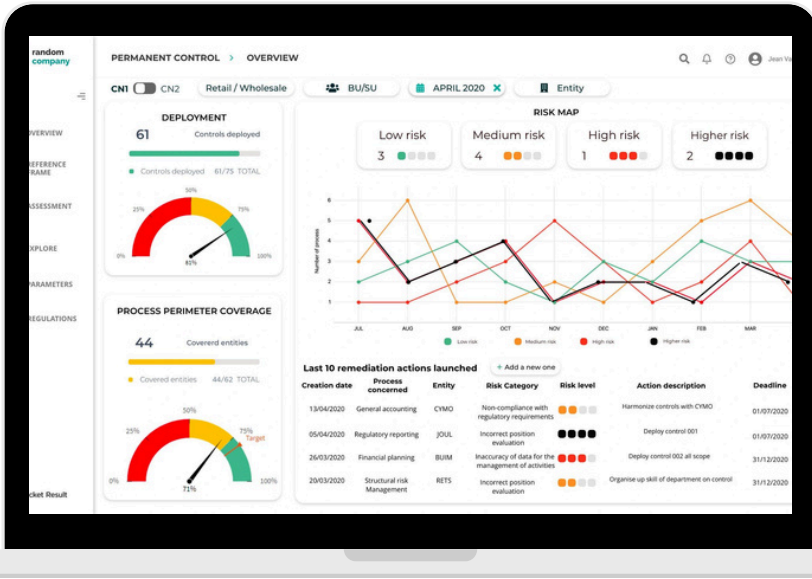
Collectez et analysez des données relatives aux incidents et menaces identifiés.

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.



Contact

Gilles CHEVILLON

+33 (0)6.65.02.73.15

gilles.chevillon@maet-consulting.com

www.maet-consulting.com

www.linkedin.com/company/maet-consulting/

Partenaires