Digital Operational Resilience Act (DORA)

L'IMPORTANCE DU **DIGITAL OPERATIONAL RESILIENCE ACT** (DORA) DANS LA CONSTRUCTION D'UNE **RÉSILIENCE NUMÉRIQUE** EUROPÉENNE

Alix VAN DEN B.
Consultante cybersécurité

A.VDB

INTRODUCTION

Le **Digital Operational Resilience Act (DORA)**, adopté par l'Union Européenne, est un **règlement** clé pour garantir la **résilience numérique des entreprises du secteur financier** face aux cybermenaces et aux perturbations technologiques.

DORA constitue une **lex specialis** de la **Directive NIS 2**, en ce sens qu'il apporte des exigences spécifiques et complémentaires en matière de résilience opérationnelle et de gestion des risques numériques pour les acteurs du secteur financier, tout en s'inscrivant dans le cadre plus large de la cybersécurité et de la protection des infrastructures critiques définies par NIS 2.

Ce règlement vise à renforcer la **gestion des risques** opérationnels, à améliorer la **résilience des infrastructures** critiques et à garantir que les entreprises financières puissent **maintenir leurs activités** essentielles en cas d'incident majeur. Il impose des obligations telles que la mise en place de plans de continuité, la gestion des prestataires tiers, ainsi que des tests réguliers de résilience, avec un **focus particulier sur la gestion des incidents** et la notification rapide des régulateurs.

En se conformant à DORA, les entreprises du secteur financier pourront non seulement **mieux anticiper et répondre aux risques**, mais aussi **garantir la stabilité et la confiance du marché** face aux défis numériques croissants.

A.VDB

01 QUI EST CORNE PAR DORA ? (ART 2)

Secteurs et acteurs concernés :

Le **Digital Operational Resilience Act (DORA)** s'applique automatiquement aux **institutions financières**, mais aussi aux entreprises de **technologies financières (fintech)**, aux compagnies d'**assurances**, ainsi qu'à leurs **prestataires de services tiers**, y compris ceux offrant des services critiques comme le cloud ou les services IT. Il est crucial que toutes ces entités, **quelle que soit leur taille**, mettent en œuvre des **mesures adaptées de résilience numérique** afin de garantir la **continuité de leurs services** face aux perturbations technologiques.

Ce règlement entrera en vigueur le **17 janvier 2025**, et aucune transposition n'est nécessaire pour sa mise en application, c'est-à-dire qu'il s'appliquera **directement aux Etats membres**.

Impact sur les PME et leurs obligations spécifiques :

Les **PME** opérant dans le secteur financier doivent adopter une stratégie de résilience numérique pour se conformer à DORA. Bien que le règlement impose des exigences strictes, il prévoit des **ajustements** permettant une **certaine flexibilité** pour les petites entreprises, notamment en termes de coûts et de ressources. Ces ajustements visent à **faciliter la mise en œuvre des mesures de résilience**, tout en garantissant la sécurité et la stabilité des services financiers.

02

GESTION DES RISQUES (CHAP 2)

A.VDB

Objectif : Identifier, évaluer et gérer les **risques liés aux technologies de l'information** (TIC) et à la **continuité des activités**.

Cartographie des risques TIC : Les entreprises doivent **identifier les risques technologiques** auxquels elles sont exposées (cybermenaces, pannes, erreurs humaines, etc.).

- *Ex : Identifier les systèmes critiques, les actifs essentiels, les vulnérabilités et les menaces potentielles via un outil de gestion des risques.*

Stratégies de gestion des risques : Mise en place de **mesures pour atténuer les risques identifiés** (par exemple, des contrôles de sécurité renforcés pour les systèmes critiques).

- *Ex : Élaborer un plan détaillant les actions à entreprendre pour atténuer chaque risque identifié. Par exemple, renforcer les mécanismes de sauvegarde des données et mettre en place une protection contre les ransomwares.*

Évaluation continue des risques : Les risques doivent être régulièrement **évalués et mis à jour en fonction des évolutions** technologiques et des menaces.

- *Ex : Implémenter un processus de revue régulière des risques, par exemple en réalisant des évaluations trimestrielles des nouvelles menaces et en ajustant les mesures de sécurité en conséquence.*

A.VDB

03 CONTINUITE DES ACTIVITES (ART 7)

Objectif : Garantir la capacité des entreprises à **maintenir leurs opérations essentielles** en cas d'**incident majeur**.

Plans de continuité des activités (PCA) : Les entreprises doivent élaborer et mettre en place des **plans détaillés pour assurer la continuité des services essentiels** en cas de perturbation majeure.

- *Ex : Rédiger un plan de continuité détaillé qui précise les actions à entreprendre pour maintenir les opérations en cas d'incident, définir des processus alternatifs pour les activités critiques en cas de panne des systèmes principaux.*

Tests réguliers : Les entreprises doivent **tester** leurs **plans de continuité** régulièrement pour s'assurer qu'ils sont efficaces en situation réelle.

- *Ex : Organiser des simulations d'incidents (tests de continuité) pour évaluer la réactivité et l'efficacité des procédures de rétablissement.*

Révision après incident : Après un incident majeur, les plans doivent être **révisés et améliorés** pour mieux faire face à des événements futurs.

- *Ex : Développer des scénarios d'urgence spécifiques aux différents types d'incidents (panne de serveur, fuite de données, cyberattaque) et tester la réponse de l'équipe avec des exercices pratiques.*

A.VDB

04 GESTION DES FOURNISSEURS SERVICE TIERS (CHAP 5)

Objectif : S'assurer que les **prestataires externes**, notamment ceux offrant des **services critiques** comme le cloud, **respectent les normes de résilience et de cybersécurité**.

Évaluation des risques tiers : Avant de collaborer avec des prestataires externes, les **entreprises doivent évaluer les risques liés à leurs services**.

- *Ex : Réaliser une évaluation de la résilience et des pratiques de cybersécurité des prestataires externes avant de conclure un contrat comme un audit de sécurité pour un fournisseur de services cloud avant de lui confier des données sensibles.*

Contrats et obligations : Les **contrats** avec les prestataires doivent inclure des **clauses** de résilience, de cybersécurité et de continuité des services.

- *Ex : Inscrire dans les contrats des exigences strictes comme une clause obligeant le prestataire à fournir des preuves de tests de sécurité réguliers et de mises à jour de sécurité pour ses systèmes.*

Surveillance continue des prestataires : Les entreprises doivent surveiller en permanence la **performance des prestataires tiers et effectuer des audits réguliers** pour vérifier leur conformité aux normes DORA.

- *Ex : Mettre en place des mécanismes pour suivre en continu les performances des prestataires externes.*

A.VDB

05 TESTS DE RESILIENCE (CHAP 4)

Objectif : **Tester** la capacité des **systèmes à résister à des cyberattaques** ou à des **pannes majeures**.

Stress tests : Les entreprises doivent effectuer des **tests de résilience** pour évaluer leur capacité à **résister à des scénarios de perturbation majeurs** (comme des cyberattaques de grande envergure).

- *Ex : Organiser des tests de résistance pour évaluer la robustesse des systèmes face à des scénarios extrêmes, comme une attaque DDoS de grande envergure ou un trafic trop intense.*

Scénarios réalistes : Les tests doivent être basés sur des **scénarios réalistes** et pertinents pour le secteur financier.

- *Ex : Simulation d'une attaque de phishing à grande échelle qui compromet plusieurs comptes utilisateurs dans l'entreprise.*

Amélioration continue : Les résultats des tests doivent être utilisés pour renforcer les systèmes et **améliorer les pratiques** de gestion des risques.

- *Ex : Après chaque test, analyser les résultats pour identifier les points faibles et ajuster les processus et les systèmes en conséquence.*

A.VDB

06 GESTION DES INCIDENTS ET NOTIFICATION (CHAP 3)

Objectif : Assurer une **gestion efficace** des **incidents** et garantir la **notification rapide** aux régulateurs et parties prenantes.

Gestion des incidents : Les entreprises doivent établir des **procédures claires pour la gestion des incidents de sécurité** ou autres perturbations majeures.

- *Ex : Mettre en place des procédures claires et documentées pour gérer les incidents de sécurité, y compris des processus d'escalade comme un protocole de communication interne pour signaler immédiatement un incident majeur.*

Notification aux régulateurs : En cas d'**incident significatif**, les entreprises doivent **notifier les régulateurs** dans les délais fixés.

- *Ex : Installer un système automatisé pour la notification des incidents aux régulateurs dans les délais prévus (souvent dans les 24 heures).*

Transparence : Les **incidents** doivent être **documentés** et **analysés** afin de tirer des **enseignements** pour améliorer les pratiques futures.

- *Ex : Après un incident, rédiger un rapport détaillé pour documenter l'événement et en tirer des enseignements pour améliorer les processus de sécurité. Analyser la cause profonde pour proposer des solutions d'amélioration continue et empêcher la reproduction de ce type d'incident.*

A.VDB

07 GOUVERNANCE STRUCTUREE

Objectif : Renforcer la **gouvernance** et la **responsabilité** en matière de cybersécurité et de **résilience**.

Responsabilité de la direction : Les dirigeants doivent s'assurer que des **politiques sécurité appropriées** sont en place et qu'elles sont suivies.

- *Ex : Nommer un responsable de la résilience numérique pour superviser la gestion des risques et la conformité aux exigences DORA.*

Rôle des responsables : Les entreprises doivent **nommer des responsables** dédiés à la gestion des risques opérationnels et à la résilience numérique.

- *Ex : Définir une structure de gouvernance pour la gestion des risques, incluant des comités dédiés à la cybersécurité et à la continuité des services.*

Révisions régulières : Les pratiques et politiques de gouvernance doivent être **révisées régulièrement** pour s'assurer qu'elles sont adaptées aux **nouvelles menaces et évolutions technologiques**.

- *Ex : Mettre en place des processus de révision régulière des politiques de gouvernance pour s'assurer qu'elles restent alignées avec les meilleures pratiques et les évolutions technologiques.*

A.VDB

08 PARTAGE D'INFORMATIONS

Objectif : **Renforcer** la **collaboration au sein du secteur financier.** Le partage d'informations vise à rendre le secteur plus résilient en assurant que les acteurs échangent des informations utiles pour mieux anticiper les menaces.

Responsabilité de la direction : Les dirigeants doivent veiller à ce que des **processus de partage d'informations** soient mis en place et que les employés comprennent l'importance de signaler les incidents de sécurité en temps réel.

Partage d'incidents de sécurité : Les entreprises doivent **notifier rapidement les incidents significatifs** aux régulateurs, et dans certains cas, à d'autres acteurs du secteur.

Échange de bonnes pratiques et de vulnérabilités : DORA encourage les entreprises à **partager des informations sur les vulnérabilités détectées** et les meilleures pratiques pour renforcer la cybersécurité.

A.VDB

09 SENSIBILISATION ET FORMATION (ART 10)

Objectif : Assurer que le **personnel** est **formé** aux **bonnes pratiques de sécurité** et à la **gestion des incidents.**

Formation continue : Les employés doivent recevoir une **formation régulière** sur la **cybersécurité**, la gestion des risques et les procédures de réponse aux incidents.

- *Ex : Offrir des formations continues sur la cybersécurité et la gestion des risques à tous les employés. Par exemple, organiser des sessions de formation annuelles sur la détection de phishing et les meilleures pratiques en matière de sécurité informatique.*

Simulation d'incidents : Des **exercices pratiques** doivent être organisés pour **tester la réaction des employés** face à des incidents en situation réelle.

- *Ex : Organiser des exercices de simulation d'incidents pour tester la réaction de l'équipe face à un scénario de cyberattaque. Par exemple, un exercice de simulation de ransomware pour évaluer la réactivité des équipes IT et des responsables de la sécurité.*

Programmes de sensibilisation : La sensibilisation doit s'inscrire dans le cadre d'un **programme avec des objectifs définis**.

- *Ex : Lancer des campagnes de sensibilisation internes pour encourager une culture de sécurité, comme des alertes régulières sur les nouvelles menaces et les comportements à adopter face à ces menaces.*

A.VDB

10

NON CONFORMITES ET SANCTIONS (CHAP 7)

La **conformité** au Digital Operational Resilience Act (DORA) est **cruciale** pour garantir la résilience numérique et la continuité des services financiers face aux cybermenaces.

Le non-respect de ces exigences peut entraîner des **sanctions financières** et des dommages à la réputation, affectant ainsi la confiance des clients et des partenaires.

Ainsi, DORA prévoit des sanctions financières en cas de non-conformité. Les **amendes** peuvent atteindre jusqu'à **2 % du chiffre d'affaires annuel mondial total** de l'entité concernée.

Les **régulateurs nationaux** auront un rôle actif en effectuant des **contrôles** pour **vérifier la conformité** des entreprises, incluant des audits et des évaluations régulières. En cas de manquements, des amendes seront appliquées **proportionnellement aux non-conformités identifiées**.

Pour les **PME**, bien que des ajustements soient prévus pour tenir compte de leurs **ressources limitées**, elles doivent tout de même **respecter les exigences fondamentales** du règlement pour éviter des sanctions et préserver la stabilité de leurs services.

A.VDB

CONCLUSION

Le **règlement DORA** représente un cadre fondamental pour la **résilience numérique** des **entreprises du secteur financier**, en visant à assurer que les services essentiels restent fonctionnels même face aux perturbations les plus sévères.

En appliquant les mesures prescrites, les entreprises peuvent non seulement se **conformer aux exigences légales**, mais aussi **renforcer leur capacité à anticiper, répondre et se remettre rapidement des cyberattaques et autres crises technologiques**.

La gestion proactive des risques, la mise en place de plans de continuité, la résilience des systèmes, et l'implication des prestataires tiers sont des étapes cruciales pour garantir la **pérennité des services financiers**.

En suivant les recommandations de DORA, les entreprises s’assurent non seulement de **protéger leurs opérations**, mais aussi de **maintenir la confiance de leurs clients** et partenaires dans un monde numérique en constante évolution.

Si ce mini guide de présentation de DORA vous a plu, n'hésitez pas à me le faire savoir et à liker et enregistrer ce post.