silex | PROTECTION DES DONNÉES ET CYBERSÉCURITÉ

Plan d'action

Mise en conformité avec le Règlement DORA

Le **Règlement DORA (Digital Operational Resilience Act)**, applicable dès le **17 janvier 2025**, impose aux entités financières de renforcer leur **résilience numérique** face aux cybermenaces. Pour assurer une mise en conformité efficace, une approche méthodique est essentielle.

Cet article vous guide à travers un **plan d'action en 15 étapes**, couvrant la **gestion des risques, la surveillance des systèmes et la réponse aux incidents**. Ne pas se conformer à DORA expose les entreprises à des **sanctions financières** et à des risques accrus pour leur sécurité numérique.

Table des matières

Étape 1 : Déterminer la pertinence du règlement DORA pour votre clientèle

Objectif

Identifier si les entités financières que vous conseillez sont concernées par DORA, en fonction de leur taille, de leur profil de risque et de la nature de leurs activités.

Actions

- ☐ Analyser **l'article 2 du règlement (UE) 2022/2554** pour identifier les entités financières soumises à DORA.
- ☐ Évaluer la **taille, le profil de risque et la complexité** des activités de vos clients pour déterminer si le **principe de proportionnalité (article 4)** peut moduler certaines exigences.
- ☐ Vérifier si vos clients sont considérés comme des **entités essentielles ou importantes** au titre de la **directive (UE) 2022/2555**, auquel cas DORA sera appliqué comme un acte juridique sectoriel.

Étape 2 : Analyser les exigences du règlement DORA

Objectif

Comprendre en détail les obligations imposées par DORA en matière de **résilience opérationnelle numérique**, de **gestion des risques liés aux TIC** et de **supervision des prestataires tiers**.

Actions

- ☐ Étudier les chapitres clés du règlement (UE) 2022/2554 :
  - **Chapitre II** : Gestion du risque lié aux TIC
  - **Chapitre III** : Gestion des incidents liés aux TIC
  - **Chapitre IV** : Tests de résilience opérationnelle numérique
  - **Chapitre V** : Gestion du risque lié aux tiers prestataires de services TIC
- ☐ Identifier les **actes délégués et d'exécution** adoptés par la Commission européenne, ainsi que les **RTS (normes techniques de réglementation)** et **ITS (normes techniques d'exécution)** élaborées par les **AES (Autorités Européennes de Surveillance)**.
- ☐ Se tenir informé des **questions-réponses (Q&R)** publiées par les AES et la Commission européenne pour clarifier l'application de DORA.

Étape 3 : Mettre en place un cadre de gestion des risques liés aux TIC

Objectif

Établir un cadre robuste, complet et documenté pour identifier, évaluer et gérer les risques liés aux TIC.

Actions

- ☐ Définir une **stratégie de gestion des risques TIC**, incluant une politique relative à l'utilisation des services TIC pour les fonctions critiques ou importantes.
- ☐ Identifier, classifier et documenter **toutes les fonctions critiques et leurs interdépendances**.
- ☐ Implémenter un **Système de Management de la Sécurité de l'Information (SMSI)** conforme à **ISO 27001**.
- ☐ Séparer clairement les **rôles et responsabilités en matière de sécurité TIC** pour éviter les conflits d'intérêts.
- ☐ Mettre en place un **cadre simplifié** pour les entités éligibles conformément à **l'article 16 de DORA**.

Étape 4 : Auditer régulièrement le cadre de gestion des risques liés aux TIC

Objectif

Vérifier l'efficacité du cadre et identifier les éventuelles lacunes.

Actions

- ☐ Effectuer des **audits internes réguliers** avec des experts en cybersécurité.
- ☐ Adopter le **modèle des Trois Lignes de Défense (3LoD)** pour assurer une gouvernance efficace.
- ☐ Documenter et analyser les résultats des audits pour améliorer continuellement le cadre de gestion des risques.

Étape 5 : Établir une stratégie de résilience opérationnelle numérique

Objectif

Assurer la continuité des opérations et la résistance aux cyberattaques et incidents majeurs.

Actions

- ☐ Élaborer une **stratégie de résilience numérique** qui inclut des mécanismes de détection, de prévention et de réponse aux incidents TIC.
- ☐ Tester et réviser la stratégie **au moins une fois par an**.
- ☐ Présenter un **rapport annuel** aux organes de direction.

Étape 6 : Mettre en place des mécanismes de détection des anomalies

Objectif

Détecter rapidement toute cybermenace ou activité anormale pour anticiper et mitiger les incidents liés aux TIC.

Actions

- ☐ **Déployer des indicateurs d'alerte précoce** : Identifier des seuils critiques (anomalies de connexion, augmentation de la charge réseau, tentatives d'accès non autorisées) déclenchant des alertes automatiques.
- ☐ **Mettre en place des systèmes de détection d'intrusion (IDS/IPS)** :
  - IDS (*Intrusion Detection System*) : Surveille et enregistre les tentatives d'attaques.
  - IPS (*Intrusion Prevention System*) : Bloque activement les intrusions.
- ☐ **Établir une veille sur les cybermenaces** :
  - Analyser en temps réel les menaces émergentes via des sources OSINT (*Open Source Intelligence*).
  - Participer à des groupes de partage d'informations sur les cybermenaces (ex. CERT, ANSSI).
- ☐ **Mettre en place une surveillance continue des systèmes** :
  - Utiliser des *Security Information and Event Management* (SIEM) pour corréler les événements et générer des alertes intelligentes.
  - Intégrer des solutions de détection basées sur l'IA pour identifier des schémas anormaux.

Étape 7 : Rédiger une politique de continuité des activités TIC

Objectif

Garantir la continuité des opérations et des services financiers en cas de perturbation ou d'incident critique.

Actions

- ☐ **Élaborer une politique complète de continuité des activités TIC** :
  - Identifier les actifs critiques (serveurs, bases de données, applications).
  - Cartographier les dépendances et interdépendances entre systèmes.
  - Définir les procédures de reprise en cas de panne ou cyberattaque.
- ☐ **Définir des objectifs de délai de rétablissement (RTO) et de point de rétablissement (RPO)** :
  - **RTO (Recovery Time Objective)** : Temps maximal d'interruption acceptable.
  - **RPO (Recovery Point Objective)** : Période maximale de perte de données admissible.
- ☐ **Tester les plans de continuité au moins une fois par an** :
  - Simuler des scénarios de panne et évaluer les capacités de réponse.

- Impliquer les équipes techniques, juridiques et opérationnelles dans les tests de reprise.

Étape 8 : Définir des procédures de sauvegarde et de rétablissement

Objectif

Assurer la protection, l'intégrité et la récupération rapide des données critiques après un incident.

Actions

- ☐ **Mettre en place des sauvegardes sécurisées et chiffrées** :
  - Utiliser des solutions de **chiffrement de bout en bout** pour garantir la confidentialité.
  - Établir une politique de sauvegarde fréquente (quotidienne, hebdomadaire, mensuelle).
- ☐ **Tester régulièrement les processus de restauration des données** :
  - Vérifier la capacité de récupération des données à partir de sauvegardes dans des environnements de test.
  - Réaliser des exercices de restauration pour évaluer les temps de réponse.

Étape 9 : Préparer des plans de communication en situation de crise

Objectif

Gérer efficacement la communication avec les parties prenantes en cas d'incident majeur pour minimiser l'impact sur la confiance et la réputation.

Actions

- ☐ **Élaborer des plans de communication de crise** :
  - Définir des messages adaptés pour les clients, régulateurs, médias et partenaires.
  - Mettre en place des protocoles pour une communication rapide et transparente.
- ☐ **Définir les rôles et responsabilités en matière de communication d'urgence** :
  - Désigner un **porte-parole officiel** pour répondre aux demandes externes.
  - Coordonner la communication avec les autorités de régulation (ACPR, CNIL, ANSSI).

Étape 10 : Établir un processus de gestion des incidents

Objectif

Assurer une réaction rapide, efficace et coordonnée face aux incidents liés aux TIC.

Actions

- ☐ **Mettre en place des procédures d'identification et de traitement des incidents** :
  - Définir un processus de signalement des incidents pour tous les employés.
  - Établir une cellule de crise dédiée à la gestion des incidents critiques.
- ☐ **Enregistrer et notifier tous les incidents majeurs aux autorités compétentes** :
  - Respecter les délais de notification définis par DORA.
  - Analyser les causes profondes et documenter les mesures correctives.

Étape 11 : Rédiger et documenter un plan de réponse aux incidents (IRP)

Objectif

Minimiser l'impact des incidents TIC en définissant des procédures claires pour la réponse et la reprise d'activité.

Actions

- ☐ **Définir un guide opérationnel en cas d'incident** :
  - Cartographier les menaces et leurs impacts potentiels.
  - Élaborer un schéma décisionnel pour les réponses à incidents.
- ☐ **Tester et mettre à jour l'IRP régulièrement** :
  - Réaliser des exercices de simulation de crise (Red Team, Tabletop).
  - Adapter le plan aux évolutions des menaces et des infrastructures TIC.

Étape 12 : Mettre en place des outils pour tester la résilience

Objectif

Évaluer la capacité à résister aux cyberattaques et incidents majeurs.

Actions

- ☐ **Réaliser des tests de pénétration (TLPT)** :
  - Identifier les vulnérabilités exploitables et corriger les failles de sécurité.
  - Mettre en place des correctifs immédiats pour renforcer la protection.
- ☐ **Identifier et corriger les vulnérabilités découvertes** :
  - Mettre en œuvre un processus de gestion des vulnérabilités pour les corriger rapidement.
  - Suivre l'efficacité des correctifs avec des audits réguliers.

Étape 13 : Former les dirigeants et employés

Objectif

Sensibiliser l'ensemble du personnel aux enjeux de cybersécurité et de conformité DORA.

Actions

- ☐ **Mettre en place des formations obligatoires** :
  - Former les dirigeants sur leurs responsabilités en matière de gestion des risques TIC.
  - Intégrer la cybersécurité dans les programmes de formation continue.
- ☐ **Organiser des exercices de simulation d'attaques** :
  - Réaliser des tests de phishing pour évaluer la vigilance des employés.
  - Simuler des attaques ransomware pour tester les capacités de réponse.

Étape 14 : Gérer les risques liés aux prestataires tiers

Objectif

Sécuriser l'externalisation des services TIC et s'assurer que les fournisseurs respectent les exigences DORA.

Actions

- ☐ **Mettre en place une politique de gestion des risques liés aux prestataires tiers** :
  - Effectuer des évaluations de sécurité avant la signature des contrats.
  - Intégrer des clauses contractuelles sur la protection des données et la continuité des services.
- ☐ **Effectuer des audits réguliers des fournisseurs** :
  - Évaluer la résilience et la conformité des prestataires stratégiques.
  - Identifier les risques de dépendance excessive.

Étape 15 : Prévoir des stratégies de sortie pour les prestataires tiers

Objectif

Anticiper le changement ou la défaillance d'un prestataire critique pour éviter toute interruption des services.

Actions

- ☐ **Élaborer un plan de sortie et de migration sécurisé** :
  - Identifier des prestataires alternatifs pour les services critiques.
  - Planifier la transition des données et applications essentielles.
- ☐ **Tester périodiquement la transition des services TIC** :

- Effectuer des tests de bascule entre prestataires.
- Évaluer les capacités internes de reprise en cas d’interruption.