Due Diligence Opérationnelle & DORA

Document mis à jour le 20/01/2025

1. Gouvernance et responsabilités

a. Mise en place de la gouvernance liée à DORA

- Quels rôles et responsabilités ont été définis au sein de votre organisation pour garantir la conformité au règlement DORA ?
- Qui est le responsable désigné pour la résilience opérationnelle numérique ?
- Pouvez-vous fournir des preuves de la formation ou de la sensibilisation des membres du conseil d'administration et des cadres dirigeants aux exigences de DORA ?

b. Politique de gestion des risques numériques

- Avez-vous élaboré une politique documentée de gestion des risques TIC (technologies de l'information et de la communication) conforme à DORA ?
- Quelle est la fréquence de mise à jour de cette politique ?
- Pouvez-vous fournir un exemple ou un extrait de cette politique ?

---

2. Identification et gestion des risques TIC

a. Évaluation des risques numériques

- Quels processus sont en place pour identifier, évaluer et documenter les risques liés aux TIC ?
- Avez-vous une cartographie des risques TIC ? Pouvez-vous la partager ?

b. Externalisation et tiers

- Quels sont vos principaux prestataires externes pour les services TIC ?
- Comment évaluez-vous les risques liés à l'externalisation des fonctions critiques (y compris la gestion des systèmes d'information) ?

- Pouvez-vous fournir les rapports de due diligence ou d'évaluation des prestataires TIC critiques ?

c. **Gestion des incidents TIC**

- Avez-vous mis en place une procédure de gestion des incidents liés aux TIC ?
- Pouvez-vous fournir un exemple de rapport d'incident récent et les actions correctives mises en œuvre ?
- Quelle est la fréquence des tests et simulations d'incidents TIC ?

---

3. Plan de continuité et de résilience opérationnelle

a. **Plan de continuité des activités (PCA)**

- Disposez-vous d'un PCA spécifique pour les systèmes TIC ?
- Quand le PCA a-t-il été testé pour la dernière fois ? Quels étaient les résultats du test ?
- Pouvez-vous fournir des copies du PCA et des rapports de tests associés ?

b. **Plan de reprise après sinistre (PRA)**

- Avez-vous un PRA en place pour vos infrastructures numériques critiques et sur vos données?
- Pouvez-vous décrire les principes de sauvegarde des données de l'entreprise (fréquence, redondance, infrastructures utilisées) ?
- Pouvez-vous fournir la documentation et les résultats des derniers tests PRA ?
- Avez-vous identifié des lacunes ou des améliorations nécessaires lors de ces tests ?

---

4. Surveillance et reporting

a. **Surveillance continue des risques TIC**

- Quels outils ou processus utilisez-vous pour surveiller en temps réel les systèmes TIC critiques ?
- Comment les alertes et incidents sont-ils escaladés au sein de l'organisation ?

b. **Rapports aux autorités réglementaires**

- Avez-vous mis en place un processus pour déclarer les incidents TIC majeurs aux autorités compétentes ?
- Pouvez-vous fournir un exemple (anonymisé si nécessaire) d'un rapport d'incident soumis à une autorité ?

c. **Tableaux de bord et indicateurs de suivi**

- Quels KPI ou tableaux de bord utilisez-vous pour suivre la conformité et la résilience TIC ?
- Comment ces indicateurs sont-ils communiqués à la direction et au conseil d'administration ?

---

5. Gestion des tiers et sous-traitants

a. **Contrats et clauses liées à DORA**

- Vos contrats avec des tiers incluent-ils des clauses spécifiques relatives à la conformité au règlement DORA ?
- Pouvez-vous fournir un exemple de contrat avec ces clauses ?

b. **Audits des tiers**

- Quelle est la fréquence des audits que vous réalisez sur vos prestataires critiques ?
- Pouvez-vous fournir des rapports ou attestations des derniers audits réalisés ?
- Pouvez-vous nous préciser si les prestataires utilisés pour la mise en place et le contrôle de vos TIC et de la sécurité de vos données ont obtenu des certifications (PASSI, SecNumCloud, ISO 27001…) ?

c. **Plans de résilience des tiers**

- Vos prestataires TIC ont-ils partagé leurs plans de résilience opérationnelle numérique ?
- Comment validez-vous leur capacité à respecter les exigences réglementaires, y compris DORA ?

---

6. Tests et simulations

a. **Tests de pénétration et cybersécurité**

- À quelle fréquence réalisez-vous des tests de pénétration sur vos systèmes TIC ?
- Pouvez-vous fournir des rapports ou résultats récents de ces tests ?

b. **Exercices de crise**

- Avez-vous réalisé des exercices de crise ou de simulation de cyberattaque récemment ?
- Quels étaient les enseignements tirés et les actions mises en œuvre suite à ces exercices ?

---

7. Documentation et preuves

a. **Archivage et accès aux preuves**

- Comment garantissez-vous l'archivage et la traçabilité des documents liés à la conformité DORA ?
- Pouvez-vous partager un échantillon de documents archivés relatifs à vos politiques TIC ou rapports d'incidents ?

b. **Contrôle interne et audits internes**

- Votre département d'audit interne réalise-t-il des revues spécifiques sur la conformité DORA ?
- Pouvez-vous fournir les rapports des derniers audits internes ?

---

8. Sensibilisation et formation

a. **Formation des employés**

- Quels programmes de sensibilisation et de formation avez-vous mis en place pour vos employés sur les exigences de DORA ?
- Pouvez-vous fournir des preuves de formation (planning, supports, attestation) ?

b. **Formation des tiers**

- Exigez-vous de vos prestataires ou partenaires qu'ils suivent des formations spécifiques pour se conformer à DORA ?