


Comment atténuer le risque de tiers pour la conformité DORA : une liste de contrôle des meilleures pratiques

Se conformer aux exigences de gestion des risques tiers de DORA implique la mise en œuvre d'une série de meilleures pratiques conçues pour identifier, évaluer et atténuer efficacement les risques. Ces meilleures pratiques de gestion des risques tiers sont des étapes concrètes que chaque professionnel de l'IT, du risque et de la conformité devrait envisager :

-  **1. Effectuez une diligence raisonnable approfondie:** Évaluez la résilience opérationnelle d'un fournisseur tiers, ses mesures de protection des données et son profil de risque global. Examinez sa stabilité financière, son historique de conformité et ses protocoles de cybersécurité également.
-  **2. Établir des contrats clairs:** Assurez-vous que tous les contrats avec des tiers incluent des clauses spécifiques concernant la gestion des risques, la protection des données et la conformité DORA. Définissez clairement les rôles, les responsabilités et les attentes.
-  **3. Mettre en place une surveillance continue:** Instaurez des mécanismes pour une surveillance continue des activités et de la performance des tiers. Cela peut inclure des audits réguliers, des évaluations de performance et une surveillance en temps réel des indicateurs clés de risque.
-  **4. Évaluer le risque périodiquement:** Effectuez des évaluations périodiques des risques pour évaluer l'impact des fournisseurs tiers sur la résilience opérationnelle de votre organisation. Cela aide à identifier de nouveaux risques et à évaluer l'efficacité des stratégies d'atténuation existantes.
-  **5. Développer des plans de réponse aux incidents:** Collaborez avec des prestataires tiers pour élaborer et tester des plans de réponse aux incidents. Assurez-vous que ces plans sont alignés avec le cadre général de gestion des incidents de votre organisation et les exigences DORA.
-  **6. Renforcez les relations solides:** Construisez et maintenez des relations solides avec vos fournisseurs tiers. Établissez et maintenez des canaux de communication ; un engagement régulier peut aider à identifier et à traiter les risques potentiels.
-  **7. Conservez une documentation détaillée:** Il est essentiel de tenir à jour des dossiers précis de toutes les activités de gestion des risques, évaluations et mesures d'atténuation. Cette documentation est cruciale pour prouver la conformité lors des audits et évaluations réglementaires.
-  **8. Révision et Mise à Jour des Politiques:** Revoyez et mettez régulièrement à jour vos politiques de gestion des risques liés aux tiers pour refléter les changements dans le paysage réglementaire, les menaces émergentes et les leçons tirées des incidents passés.