Loi DORA et gestion des risques liés aux tiers

Maintenir la résilience du secteur financier européen en cas de graves perturbations opérationnelles

Pour faire face à la multiplication des cyberattaques, l'UE a adopté une législation visant à renforcer la sécurité informatique des entités financières. La loi sur la résilience opérationnelle numérique (DORA, ou « Digital Operational Resilience Act », en anglais) crée un cadre réglementaire en faveur de la résilience opérationnelle numérique, en vertu duquel tous les établissements financiers doivent confirmer qu'ils sont en mesure de résister face à un large éventail de perturbations des technologies de l'information et de la communication (TIC) et de cybermenaces, ainsi que d'y répondre et de rétablir leur activité.

Principes relatifs à la gestion des risques liés aux tiers et articles figurant dans la loi DORA

La présente synthèse examine les principaux articles de la réglementation DORA connexes aux tiers et identifie les capacités en matière de meilleures pratiques permettant de répondre aux exigences imposées par cette loi.

Article 25 : Principes généraux

Exigences : l'article 25 stipule que « les entités financières gèrent les risques liés aux tiers dans le domaine des TIC comme une composante à part entière des risques TIC dans leur cadre de gestion des risques TIC et conformément aux principes suivants » : gestion des contrats, criticité des tiers, rapports, diligence raisonnable précontractuelle, audits et stratégies de sortie.

Téléchargez la liste de contrôle complète (en anglais) de la conformité à la loi DORA, à l'adresse :

https://www.prevalent.net/content-library/dora-third-party-compliance-checklist/

Recommandations : afin de répondre aux exigences énoncées à l'article 25, il est nécessaire d'automatiser les processus d'identification, évaluation, gestion, surveillance continue, création de rapports et remédiation des risques des tiers, liés à la sécurité informatique, à la protection de la vie privée, à la conformité, à l'exploitation et aux achats/à la chaîne d'approvisionnement, tout au long du cycle de vie des fournisseurs, en recourant à un cadre réglementaire commun tel que la norme ISO 27001. Pour ce faire, il conviendra d'intégrer les évaluations, la gestion des demandes de soumission (RFx), la gestion du cycle de vie des contrats et le suivi des risques dans une solution unique, afin d'unifier les processus et d'étendre la visibilité des risques à l'ensemble de votre institution, conformément aux efforts de gestion des risques au sens large.

Article 26 : Évaluation préliminaire des risques de concentration des TIC et accords de sous-traitance supplémentaires

Exigences : l'article 26 comprend des dispositions visant à guider les entités dans l'évaluation des risques de concentration et des risques associés aux différents prestataires utilisés par les tiers (quatrième à Nième niveaux), notamment des recommandations pour la surveillance des risques et les exigences contractuelles.

Recommandations : atténuer les risques de concentration en identifiant les relations avec les prestataires utilisés par les tiers, par le biais d'une évaluation des fournisseurs ou d'une analyse passive de l'infrastructure publique du tiers concerné. La carte des relations qui en résulte décrit les chemins d'information et les dépendances qui pourraient ouvrir des voies d'accès à un environnement. Recueillir des renseignements sur les fournisseurs afin d'identifier les risques financiers, environnementaux, sociaux et de gouvernance (ESG), cyber, commerciaux et de violation de données, ainsi que pour découvrir les sanctions et les personnes politiquement exposées (PPE) liées à chaque entreprise dans votre vaste écosystème de fournisseurs.

Article 27 : Principales dispositions contractuelles

Exigences : l'article 27 comprend des conseils permettant de s'assurer que les contrats avec les fournisseurs tiers comprennent des droits et des obligations qui peuvent être évalués en permanence.

Recommandations : centraliser la distribution, la négociation, la rétention et la révision des contrats avec les fournisseurs, grâce à un processus de travail permettant d'automatiser le cycle de vie des contrats, de l'intégration à la résiliation. Simplifier le processus de gestion et de surveillance des contrats avec les fournisseurs, des lignes rouges, des dates et d'autres attributs clés, afin de garantir la mise en place et le suivi des principales dispositions contractuelles jusqu'à leur aboutissement.

Article 28 : Désignation des prestataires de services tiers pour les technologies TIC critiques

Exigences : l'article 28 identifie les principaux critères que les entités doivent prendre en compte afin de désigner comme « critiques » leurs prestataires de services tiers.

Recommandations : classer automatiquement les prestataires par niveau en fonction de leur criticité quant aux opérations commerciales, en procédant à une évaluation des risques inhérents. Les résultats peuvent être utilisés pour fixer des niveaux appropriés de diligence raisonnable supplémentaire et pour déterminer la criticité et la portée des évaluations en cours.

Article 29 : Structure du cadre de supervision

Exigences : l'article 29 décrit comment mettre en place et administrer un programme de gestion des risques liés aux tiers, en identifiant notamment les rôles essentiels.

Recommandations : élaborer un programme complet de gestion des risques liés aux tiers (TPRM), fondé sur les meilleures pratiques éprouvées et une vaste expérience du monde concret. Pour être complet, un tel programme doit s'étendre de la définition des processus TPRM à la sélection des questionnaires d'évaluation et des cadres réglementaires, en passant par l'évaluation et l'optimisation continues du programme TPRM afin de couvrir l'ensemble du cycle de vie des risques liés aux tiers.

Article 32 : Demande d'information et Article 33 : Enquêtes générales

Exigences : les articles 32 et 33 expliquent comment mener des audits et autres enquêtes connexes, y compris comment identifier les types de données à recueillir.

Recommandations : mettre en place un programme permettant d'atteindre et de démontrer efficacement la conformité, en recueillant et en quantifiant les informations sur les risques liés aux fournisseurs, en recommandant des mesures correctives et en produisant des rapports conformes à la norme ISO 27001.

Article 34 : Inspections sur site

Exigences : l'article 24 décrit les processus d'examen et d'audit des contrôles effectués sur site.

Recommandations : examiner les réponses et la documentation des évaluations de tiers par rapport aux protocoles de test établis, afin de valider la mise en place des contrôles indiqués. Mettre en correspondance les réponses avec les cadres de contrôle communs, tels que la norme ISO 27001, afin de simplifier la création de rapports. Établir des plans de remédiation et en assurer le suivi jusqu'à leur achèvement.

Article 35 : Supervision continue

Exigences : l'article 35 décrit les processus de gestion continue d'un programme de gestion des risques liés aux tiers, notamment la surveillance continue et les obligations de communication régulière de rapports aux autorités compétentes.

Recommandations : suivre et analyser en permanence les menaces externes qui pèsent sur les tiers. Surveiller Internet et le Dark Web afin de détecter les cybermenaces et les vulnérabilités, et surveiller également les sources publiques et privées d'informations relatives à la réputation, aux sanctions et aux finances. Intégrer et mettre en corrélation les informations tirées de la surveillance continue avec les résultats de l'évaluation, afin de disposer d'un emplacement central permettant de visualiser les risques et d'agir en conséquence, et de fournir des rapports aux auditeurs et autres parties prenantes.