

Stratégies pratiques pour mise en œuvre de conformité DORA

Comprendre le contexte et les objectifs de DORA

Stabilité financière, Continuité et réglementation des secteurs financiers

- La réglementation prudentielle : assurer et renforcer la solidité et la stabilité du système financier mondial
- Les risques opérationnels, informatiques et de continuité parmi les menaces à la stabilité du système financier
- Les risques de non conformité à DORA - Quelles sanctions ? Quelles sont les modalités de contrôle et quel est le rôle de l'ANSSI et des autorités bancaires ?
- Aperçu de DORA et de son importance dans la réglementation financière de l'UE
- Explication de la raison pour laquelle DORA a été votée et de ses objectifs
- Exercice : Quizz

Un réveil !

- Une préoccupation de toujours pour les infra structures de paiement
- Un réveil récent pour les établissements (banques, ...)
- Livre blanc sur le risque informatique CB 1984
- Arrêté du 3 novembre 2014 sur le contrôle interne
- EBA GL on ICT and Security Risk Management 2019
- Note de l'ACPR sur le risque informatique 2021
- Un avis mitigé de IEIOPA pour les assureurs

Dispositions clés de DORA

- Cadre de gestion des risques liés aux TIC
- Gestion, classification et déclaration des incidents liés aux TIC
- Tests de résilience opérationnelle numérique
- Gestion des risques des tiers des TIC
- Partage d'informations et de renseignements
- Politique sur les arrangements avec les fournisseurs de services tiers en TIC
- Exercice : Discussion sur les implications de ces dispositions pour les institutions financières.

Mettre en oeuvre DORA

Chacun à son poste

- Rôle de la Gouvernance des établissements
- Comprendre et Comparer
- Questionner et Evaluer
- Suivre et Orienter
- Responsabilités de l'organe de direction
- Examen des responsabilités spécifiques de l'organe de gestion comme indiqué dans DORA. (En particulier à l'article 5) : formation, attention particulière, action sur les composantes clés de la gestion des risques TIC, ...
- Pilotage du projet DORA pour assurer la conformité et la résilience opérationnelle.
- Contribution des services concernés :
 - Responsables Achats / Externalisation et juridique
 - Directions informatiques
 - RSSI, auditeurs et contrôleurs internes
- Exercice : qui fait quoi ?

Démarches de Mise en oeuvre

- Stratégies pratiques pour la mise en oeuvre de la conformité DORA au sein des institutions financière :
 - faire / faire faire
 - big bang / amélioration continue
 - ciblage / globalisation
 - attente / proactivité
 - Plan d'actions de mise en oeuvre
- Accompagnement non technique :
 - Orienter l'établissement : actions de gouvernance, politiques et canaux de communication adéquats.
 - Favoriser une culture de la résilience opérationnelle numérique au sein de l'organisation.
- Exercice : Quizz

VALIDATION DES ACQUIS PAR QUIZ