FORMATION

Programme de Formation

Être en conformité avec les textes DORA (Digital Operational Resilience Act)

Organisation

Durée : 7 heures

Mode d'organisation : Présentiel

Contenu pédagogique

Public visé

Responsables de la conformité et de la réglementation.

Responsables des risques opérationnels.

Directeurs des technologies de l'information (IT).

Directeurs de la sécurité de l'information (DSI).

Juristes spécialisés en droit bancaire et en droit des technologies de l'information.

Responsables de la gestion des contrats avec les fournisseurs de services TIC.

Objectifs pédagogiques

- Maîtriser les contraintes de la résilience opérationnelle et de la continuité d'activité en gestion des risques TIC
- Connaitre les aspects contractuels et légaux dans le cadre de DORA
- Superviser efficacement les risques TIC et les entités impliquées dans DORA

Description

1.Le contexte : La notion de « résilience opérationnelle » : assurer la continuité de l'activité
- Le dispositif de gestion des risques liés aux TIC
- La gestion et le reporting des incidents TIC et des cybermenaces
- Les tests de la résilience opérationnelle numérique
- La gestion des risques liés aux prestataires de services TIC
- Le partage d'informations en matière de cybersécurité
- Le périmètre : les personnes assujetties

Les prestations TIC
L'application territoriale :
- le groupe de sociétés et les prestations TIC intragroupe
- les fournisseurs de pays tiers

L'application dans le temps
La contractualisation (2h)
Les obligations contractuelles impératives
- clauses obligatoires
- clauses à « envisager »

Les clauses standard UE à venir : leur valeur impérative limitée
L'analyse d'écart avec les PCI/PSEE et les guidelines EBA sur les accords d'externalisation de février 2019La

négociation et la forme du contrat

2. Les risques TIC :

- Caractérisation et articulation avec les stratégies et politiques IT : lien avec l'arrêté du 3 novembre 2014 remanié en 2021
- La gouvernance interne et les organes sociaux de l'entité financière bénéficiaire
- Les tests de pénétration et autres contrôles, LOD 1 et LOD2
- La décision de remontée des menaces ou incidents aux superviseurs, articulation avec d'autres obligations (DSP2, etc.). Les perturbations du système IT et l'alerte du secteur bancaire et financier.
- La remédiation

3. La supervision : La supervision de l'entité financière bénéficiaire

- Le registre
- Le lien avec le cadre de supervision des prestations externalisées essentielles, critiques ou importantes
- Les TIC dans le plan de rétablissement et de résolution
- Les reportings

La supervision du fournisseur critique

- La détermination de l'autorité compétente
- Les pouvoirs de l'autorité compétente

-Les contrôles, enquêtes et sanctions

Prérequis

Avoir des notions sur les prestations IT et sur la contractualisation des externalisations

Modalités pédagogiques

- Présentiel
- Remise des supports de formation
- Formation interactive et pratique : présentation théorique, cas pratiques, quizz