COMPTABILITE, GESTION, FINANCE

FICHE PROGRAMMATION

AFGES - DORA : QUELLES EXIGENCES, QUELS IMPACTS POUR VOTRE ORGANISATION

Public

Auditeur(trice),Auditeur(trice) interne,Chargé(e) de mission,Directeur(trice) et responsable d'équipe,Directeur(trice)/Responsable administratif(ve) et financier (e)

Prérequis

Aucune connaissance particulière n'est exigée.

Objectifs pédagogiques

Connaître le dispositif réglementaire DORA.
- Identifier les principaux impacts par rapport aux règlementations existantes.
- Se préparer aux nouvelles exigences en capitalisant sur l'existant.
- Comprendre les nouveaux enjeux de supervision.
- S'appuyer sur les meilleures pratiques de place.

Contenu

PARTIE 1 : ENJEUX ET CONTEXTE REGLEMENTAIRE

Enjeux du risque Cyber pour l'industrie bancaire européenne.

Limites actuelles du cadre réglementaire européen.
Risque Opérationnel vs Résilience Opérationnelle
Contexte réglementaire du règlement DORA :
- Principales définitions.
- Périmètre des entités concernées.
- Présentation synthétique des obligations :
Gestion du risque informatique, des incidents informatiques, tests de résilience et gestion du risque de tiers.
Calendrier d'application.
Travaux réglementaires à venir (2023/2025).
Lien et interactions avec les réglementations existantes (NIS2, SRI2, DSP2, Arrêt, DSP2, Arrêté du 3 novembre 20214, etc.).

PARTIE 2 : GESTION DU RISQUE INFORMATIQUE

Principes de Gouvernance du risque.
Rôles de l'Organe de Direction selon DORA.
Stratégie de résilience opérationnelle numérique.
Cadre de gestion du risque informatique.

PARTIE 3 : GESTION DES INCIDENTS INFORMATIQUES

Processus de gestion des incidents informatiques.
Classification des incidents liés à l'informatique selon DORA :
Taxonomie de référence de l'ENISA.
Classification des incidents IT du Groupe d'Experts en Sécurité du G7.
Principes de notification des incidents informatiques majeurs aux autorités :
Reportings et échange d'informations.
Interactions entre DORA/SRI2 et DSP2.

PARTIE 4 : TESTS DE RESILIENCE

Principes du programme de tests de résilience opérationnelle numérique.
Approche par les risques et principes de proportionnalité.
Tests de pénétration avancés fondés sur la menace (TLTP) :
- Couverture des fonctions critiques ou importantes.
- Participation des prestataires de services tiers.
- Principes de reconnaissance mutuelle au niveau européen.

- Conditions à respecter pour les testeurs internes et externes.
Intégration dans les dispositifs de tests existants en matière de sécurité des SI, Continuité d'Activité et Gestion de Crise.

PARTIE 5 : GESTION DU RISQUE DE TIERS

Périmètre.
Gestion des risques liés aux prestataires.
Obligations contractuelles.
Registre d'informations.
Suivi de la performance et de la qualité.
Cadre de surveillance des prestataires critiques par les AES.
Analyse comparée des obligations DORA vs Guidelines de l'EBA en matière d'Outsourcing de Prestations Critiques vs Arrêté du 3 Novembre 2014 sur les PSEE.