Le règlement DORA, vos Tiers TIC et votre registre d'informations sous contrôle

PROCHAINE SESSION :

- Le 24/04/2025

PUBLIC :

Dirigeants d'établissements financiers, DSI, RSSI, Direction des Risques et du Contrôle Interne, Directions Juridiques et des Achats

Chefs de projets, consultants et prestataires de services –

Toute personne au sein des institutions financières en charge de mettre en œuvre des accords contractuels avec des tiers prestataires de TIC

PRÉ-REQUIS :

Aucun

APPROCHE PÉDAGOGIQUE :

La formation s'appuiera sur un exposé pédagogique mis en contexte, enrichi par des quizz et des exercices de mise en situation

MODALITÉS D'ÉVALUATION :

Une évaluation des acquis sera réalisée à l'issue de la formation

Remise d'une attestation individuelle de formation

Durée

Une journée soit 7 heures
(De 9 heures à 17 heures)

Tarif de la formation

1 000 € HT

Objectifs pédagogiques

Comprendre la réglementation DORA en donnant les clés essentielles pour structurer une mise en conformité efficace.

Structurer de manière détaillée le pilier de gestion des prestataires de TIC au sein de votre entreprise.

Anticiper et élaborer une résilience opérationnelle liée aux tiers TIC notamment cloud en garantissant une gestion de la relation avec les prestataires alignée sur les exigences des régulateurs.

Intervenants

Fabrice Rosa

Après un début de carrière au début des années 2000, Fabrice a exercé ces dernières années des fonctions de directeur de projet et de DSI pour plusieurs banques et mutuelles d'assurance. Il intervient en tant que consultant et manager de transition auprès de directions évoluant dans les secteurs de l'assurance et de la prestation de conseil ou de services informatiques. Il est aussi l'auteur de l'ouvrage « Gérer les risques informatiques dans le secteur financier, Mettre en œuvre la réglementation DORA ».

Hélène Dufour

Spécialiste de la Gestion des Risques Numériques et des réglementations prudentielles (CRD IV, Solvabilité 2) Hélène est associée du Cabinet Metametris, elle intervient dans des missions d'implémentation de DORA auprès de Banques d'Assureurs et de Mutuelles). Au cours de ses missions elle a développé une bibliothèque de documents de référence (politiques, procédures, méthodologies) pour permettre à ses clients de se mettre en conformité avec DORA. Elle est certifiée LSTI ISO/IEC 27001 Lead Auditor et Lead Implementer et ISO/IEC 27005 Risk Manager.

Programme de la Formation

Partie I : Présentation de la réglementation

Introduction à la réglementation DORA

- Historique et contexte de DORA
- Les entités et prestataires concernés
- Le principe de proportionnalité
- Les sanctions

Gouvernance

- La Gouvernance
- Les 3 lignes de Défense
- Le Cadre de Gestion des Risques
- Ce qui est attendu par l'ACPR & l'AMF

Gestion des risques IT

- La Stratégie de résilience
- Gestion des actifs & des processus
- Positionnement & valorisation du SI
- DORA & ITIL V4
- L'amélioration continue et la sensibilisation

Gestion Des Incidents IT

- Les Exigences de la gestion des incidents
- Identification et notification des incidents majeurs à l'ACPR

Tests de Résilience & Sécurité SI

- Les objectifs des tests de résilience
- Les tests de résilience avancés (TLPT) êtes-vous concernés ?

Gestion des risques liés à vos prestataires

- La gestion des risques liés aux prestataires de TIC
- Les 5 principes clés de la gestion des prestataires
- Les responsabilités et les exigences à l'entrée en relation avec un prestataire de TIC
- Le cycle de vie et la mise en conformité des accords contractuels

Partie II : La construction du registre d'informations et l'évaluation des risques liés aux tiers TIC

Présentation du registre

- Vue d'ensemble du registre d'informations
- La gestion de la chaîne d'approvisionnement en TIC
- Éléments du registre issus des contrats
- Éléments du registre issus des BIA
- Méthodologie de construction des BIA alignée par rapport à DORA

Comment identifier et évaluer les fonctions critiques ou importantes ?

- Identification des fonctions critiques ou importantes au sens de DORA dans les BIA
- Échelle d'impact et appétence au risque
- Évaluation de la DMIA (RTO) et de la PDMA (RPO) d'une fonction
- Identification et classification des actifs de TIC

Comment évaluer la dépendance par rapport aux actifs de TIC ?

- RPO/RTO et niveau de dépendance des fonctions par rapport aux actifs TIC
- Substituabilité et possibilité de réintégration d'un service TIC
- Évaluation du niveau de confidentialité de l'information
- Évaluation du besoin d'intégrité des données
- Évaluation du besoin d'authenticité et de traçabilité des données
- Utilité des RTO/RPO et de l'évaluation DICA du point de vue de la maîtrise des risques

Comment évaluer les risques liés aux prestataires TIC ?

- Vue d'ensemble des risques liés aux prestataires TIC
- Identification et évaluation des risques à l'entrée en relation avec les tiers TIC
- Le risque de défaillance d'un tiers et la stratégie de réversibilité
- Zoom sur les risques de sécurité et utilisation de la méthode EBIOS RM
- Illustration : l'affaire Solarwinds, une attaque de la supply chain emblématique
- Évaluation des causes : sources de risque et objectifs visés
- Évaluation des risques liés à l'écosystème
- Identification des scénarios stratégiques
- Étude d'impact : utilisation des résultats des BIA et prise en compte de l'appétence au risque
- Traitement du risque et dispositifs de maîtrise
- Processus d'acceptation du risque
- Exercice : étude d'impact d'un scénario de défaillance d'un prestataire.

Retours d'expériences

- Étude d'impact de la mise en conformité des tiers TIC auprès d'acteurs financiers
- Synthèse des retours d'expérience
- Et chez vous quelles sont les questions qui se posent ?