Formation « DORA Lead Implementer »

Comprendre et implémenter DORA

Réf : DORALI

Cette formation a été conçue par des experts reconnus du droit et de la cybersécurité (technique aussi bien qu'organisationnelle) afin de comprendre, appréhender et implémenter les exigences issues du Règlement DORA, des textes réglementaires qui l'accompagnent, des règlements et directives ayant un rapport avec la résilience opérationnelle numérique, ainsi que de la production des superviseurs, nationaux et européens, sur ce sujet.

La présentation de cet ensemble réglementaire, au travers de sessions interactives et de cas pratique servant de fil rouge à l'ensemble de la formation, a pour but de :

- **Remettre les exigences de cyber résilience dans leur contexte plus global, aussi bien français qu'européen, et comprendre les enjeux, à l'heure de la multiplication des textes afférents aux mesures de sécurité (objets connectés, infrastructures connectées, données sensibles, éditeurs de logiciels, plateformes, etc.) ;**
- **Comprendre les articulations entre le Règlement DORA et les textes qui lui sont connexes, bien qu'ayant un domaine d'application différent ;**

Appréhender le texte du Règlement, mais également ses textes d'application (normes techniques réglementaires - RTS et normes techniques d'implémentation - ITS) ;
Anticiper les étapes nécessaires à la conduite d'un programme d'implémentation du règlement ;
Donner toutes les clés de la mise en conformité, non seulement à destination des entités du secteur financier, mais aussi vers les entités prestataires participant à la chaîne d'approvisionnement de ces dernières ;
Appréhender les mécanismes de supervisions s'appliquant aux prestataires TIC critiques
Analyser et savoir implémenter en pratique les notions clés de DORA : gestion des risques, gestion des vulnérabilités, notification des incidents de sécurité, formation des personnels et des dirigeants, communication, résilience, gestion de la relation contractuelle avec les tiers, rétablissement, conduite des tests, rédaction de rapports etc … ;
Comprendre les activités récurrentes à mettre en œuvre sous forme de processus afin de pérenniser la gestion des risques et les pratiques de cyber résilience opérationnelle en respect des exigences de la directive
Formaliser un gap-analysis et son plan d'actions à partir d'une situation existante exploitant les référentiels connus (RGPD, ISO 27001 et 27002, Guide d'hygiène de l'ANSSI, Framework du NIST, HDS, LPM…).

Tout comme la formation, ce descriptif sera mis à jour pour intégrer les dernières actualités (ANSSI, réglementation, travaux parlementaires réglementaires).

Objectifs

- **Vous doter des connaissances et des compétences nécessaires à la compréhension et à l'implémentation des exigences issues du Règlement DORA, vous permettant de planifier, réaliser, gérer, maintenir et mettre à jour votre conformité dans ce domaine.**

Durée & horaires

- **3 jours, soit 21 heures de cours et un examen de certification le vendredi après-midi**
- **Horaires : du lundi au jeudi : de 9h30 à 12h00 et de 13h30 à 18h00**

Nombre de participants

- **Minimum 6 participants – Maximum 16 participants**

Public visé

- **Professionnel de la cybersécurité ayant à prendre en charge ou à mettre en œuvre la conformité de leur organisme aux exigences issues du Règlement DORA**
- **Décideur soucieux de connaître les exigences issues du Règlement DORA**
- **RSSI et leurs équipes**
- **Personnes responsables de services opérationnels**
- **DSI et leurs équipes**
- **Responsables méthodes et qualité**
- **DPO, DRPO**
- **Juristes et responsables juridiques**
- **Responsables de conformité**
- **Responsable risque opérationnel**

Prérequis

- **Avoir une connaissance des principes de sécurité de base (qui ne seront pas réabordés pendant la formation), par exemple avoir suivi la formation SECUCYBER**

Méthodes pédagogiques

La méthode pédagogique se fonde sur les quatre axes suivants :

- **Un cours magistral fondé sur le Règlement DORA et ses textes de transposition en droit français, ainsi que sur les textes officiels et normes techniques ayant des interactions fortes avec ce cadre réglementaire (RGPD, NIS 2, Normes ISO 27XXX, etc.) ;**
- **Enrichi de cas pratiques et d'exemples concrets illustrant les notions explicitées profitant du partage d'expérience des instructeurs HS2 tous avocats ou consultants spécialistes reconnus de ces questions ou implémenteurs des normes 27001 ou encore 27701 ;**
- **Exercices de contrôle des connaissances sur les concepts à connaître pour évaluer le niveau de compréhension et de connaissance ;**
- **Un cas pratique d'implémentation servant de fil rouge à l'ensemble de la formation qui permettra de dérouler un projet complet de mise en conformité.**

Matériel

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Feuilles d'émargement par demi-journée de formation et certificat individuel de formation attestant de la participation à l'ensemble de la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation prépare à l'examen de certification HS2 DORA Lead Implementer. A l'issue de cette formation, le stagiaire passe l'examen d'une durée de 2h00 en français. L'examen sous forme de QCM est constitué d'une partie dédiée aux notions de cours et d'une partie de mise en situation via une étude de cas.**

Programme *(Proposition)*

Jour 1 - Introduction et contexte du Règlement DORA

- Le droit européen
- Qu'est-ce qu'un règlement ?
- DORA et les RTS / ITS
- Les acteurs visés par DORA
- Le calendrier de DORA : les attentes des superviseurs en termes de rapports
- L'articulation de DORA avec les autres dispositifs réglementaires :
  - RGPD
  - RGS – LPM (sous réserve du projet de loi Résilience)
  - NIS1 / NIS 2
  - CER - CRA
  - Normes (ISO – NIST) évoquer l'impact du droit souple
  - Schemes EUCS - EUCC
  - Référentiel ACPR (arrêté contrôle interne)
  - Normes des superviseurs (ANSSI – CNIL – ACPR - EBA...)
  - Le cyberscore
  - La veille techno et réglementaire – Une obligation
  - La cyber résilience v/s la cybersécurité
- Les pouvoirs des autorités prévus par DORA
- Présentation générale des 5 Piliers du Règlement DORA
  - Gestion des risques liés aux TIC
  - Gestion des incidents liés aux TIC
  - Tests de résilience opérationnelle numérique
  - Gestion des risques liés aux prestataires de services TIC
  - Partage d'informations liés aux cybermenaces

Jour 2 – Comprendre le Règlement DORA

- **Présentation détaillée du Pilier Gestion des risques liés aux TIC**
  - Objectifs et exigences de niveau 1 et 2
  - Définitions (Services TIC, prestataires de services TIC …)
  - Formation et sensibilisation des dirigeants et personnels
  - DORA et l'approche par les risques
  - Les trois lignes de défense
  - Cadre général de gestion des risques
  - Cadre simplifié de gestion des risques
  - Cartographie des systèmes financiers et d'information
  - Gestion de la continuité des services TIC
  - Chiffrement et contrôles cryptographiques
  - Gestion des clés cryptographiques

- Gestion des vulnérabilités et correctifs
- Sécurité des données et des systèmes
- Gestion de la sécurité des réseaux
- Gestion de l'identité et contrôle d'accès
- Sécurisation des informations en transit
- Détection et réponse
- Sécurité physique et environnementale

- **Présentation détaillée du Pilier Gestion des incidents liés aux TIC**
  - Objectifs et exigences de niveau 1 et 2
  - Critères et seuils de classification
  - Processus de classification des incidents majeurs
  - Processus de notification et de reporting des incidents majeurs
  - Notification des cybermenaces significatives
  - Estimation des coûts et pertes annuels agrégés

- **Présentation détaillée du Pilier Tests de Résilience Opérationnelle**
  - Objectifs et exigences de niveau 1 et 2
  - Programme des tests de résilience opérationnelle
  - Tests de pénétration fondés sur la menace (TLPT)

- **Présentation détaillée du Pilier Gestion des risques liées aux prestataires de services TIC**
  - Objectifs et exigences de niveau 1 et 2
  - Encadrement contractuel
  - Supervision par les ESAS de prestataires critiques
  - Surveillance des prestataires par les entités financières
  - Registre d'information

- **Présentation détaillée du Partage d'informations**
  - Objectifs et exigences
  - Partage d'informations des prestataires tiers de services TIC

Jour 3 – Implémenter le Règlement DORA et examen

- **Implémenter le Règlement DORA pour une entité financière**
  - Construire un référentiel d'exigences DORA
  - Conduire une démarche de cadrage de la conformité à DORA
  - Construire un programme de conformité DORA
  - Impliquer les parties prenantes dans la conformité DORA
  - Sensibiliser et communiquer autour de DORA
  - Implémenter les exigences du pilier Gestion des risques liés aux TIC
  - Implémenter les exigences du pilier Gestion des incidents liés aux TIC
  - Implémenter les exigences du pilier Tests de Résilience Opérationnelle
  - Implémenter les exigences du pilier Gestion des risques liées aux prestataires de services TIC
  - Implémenter les exigences du pilier Partage d'informations
  - Mesurer son niveau de conformité et construire les indicateurs de conformité
  - Préparer un audit de conformité du ré
  - Organiser et piloter le maintien de la conformité
  - Organiser la relation avec les régulateurs
  - Les facteurs clés de succès de la conformité DORA

- **Implémenter le Règlement DORA pour un prestataire de services TIC**
  - Organiser sa relation avec ses clients du secteur financier

- Organiser sa relation avec les régulateurs pour les prestataires critiques
- Se préparer aux évolutions contractuelles
- *A compléter*

- **Examen**