DORA (Digital Operational Resilience Act), Implement a digital resilience strategy

Durée: 2 Jours **Réf de cours: DORA** **Version: 1**

Résumé:

Le référentiel DORA est un cadre réglementaire européen visant à renforcer la résilience opérationnelle des entités financières face aux risques liés aux technologies de l'information et de la cybersécurité.
Il impose des exigences strictes en matière de gestion des risques IT, de tests de cybersécurité, de gestion des incidents, et de résilience des infrastructures critiques.
En harmonisant les standards à l'échelle de l'UE, DORA assure une protection accrue contre les cybermenaces, limitant les interruptions des services financiers et renforçant la confiance numérique.
Mise à jour : 13/10/2025

Public visé:

RSSI et référents sécurité, architectes sécurité, directeurs et responsables informatiques, ingénieurs IT, chefs de projet (MOE, MOA), auditeurs de sécurité et juristes réglementaires IT.

Objectifs pédagogiques:

- À l'issue de la formation, le participant sera en mesure de :
- Comprendre les principaux objectifs et concepts clés du règlement DORA
- Connaître les différents types de cyber-risques
- Identifier les obligations en matière de sécurité des données et de conformité réglementaire
- Appréhender les bonnes pratiques de sécurité numérique et sensibiliser les collaborateurs
- Mettre en place et établir une stratégie de résilience numérique

Pré-requis:

Connaissances de base en cybersécurité et sécurité des systèmes d'information.

Contenu:

Module 1 : Gestion des risques liés aux technologies de l'information et de la communication (TIC)

- Dispositions DORA rappelant la nécessité de mettre en œuvre un dispositif de gestion des risques liés aux TIC.
- Principes et exigences clés en matière de gestion des risques des entités financières.
- Obligations relatives au cadre de gestion des risques liés aux TIC.

Module 2 : Gestion, classification et déclaration des incidents liés aux TIC

- Dispositions du règlement DORA visant à harmoniser et à rationaliser la notification des incidents liés aux TIC.
- Classification et notification des incidents liés aux TIC.
- Notification aux autorités compétentes AES (Autorités européennes de surveillance) des incidents majeurs liés aux TIC.
- Notification, à titre volontaire, des cybermenaces importantes aux autorités comme l'EBA, l'EIOPA et l'ESMA.

Module 3 : Les tests de résilience opérationnelle numérique

- Tests de résilience opérationnelle numérique sur les parties les plus critiques de leur système d'information.
- Tests avancés basés sur des tests de pénétration fondés sur la menace (Threat-Led Penetration Testing – TLPT).
- Tests en direct à grande échelle sur les menaces, effectués par des organismes testeurs indépendants

Module 4 : Gestion des risques liés aux prestataires tiers de services

- Principes relatifs à la gestion des risques liés aux tiers dans le cadre de la gestion des risques liés aux TIC.
- Dispositions à prendre en compte dans la relation avec les prestataires de services tiers fournissant des services TIC.
- Cadre de surveillance à l'échelle européenne pour les prestataires tiers critiques de services TIC.

Module 5 : Dispositions relatives à l'échange d'informations

- Renforcer la résilience opérationnelle numérique des entités financières.
- Échange volontaire d'informations et de renseignements sur les cybermenaces entre les différentes entités financières.

Méthodes pédagogiques :

Modalités d'évaluation
Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises. Exercices pratiques a chaque étape de la formation. Etude de cas permettant de relier les différents blocs de compétences. Quiz de validation des acquis a la fin de chaque journée de formation. Auto-évaluation des acquis par le stagiaire via un questionnaire.
Méthode pédagogique :
La formation repose sur une combinaison équilibrée d'approches théoriques et pratiques, garantissant à la fois l'acquisition de connaissances et leur application ope rationnelle : Apports théoriques structures, illustrés par des exemples concrets et adaptés au contexte professionnel des participants. Exercices pratiques à chaque étape pour favoriser l'appropriation des connaissances. Etude de cas permettant de relier les différents blocs de compétences. Forte interaction entre les formateurs et les stagiaires permettant de rendre les échanges plus concrets, en corrélation avec les attentes des stagiaires. Documentation pédagogique compléte, fournie au format papier ou numérique.
Profil du formateur :
Consultant-Formateur expert en conformité réglementaire et résilience opérationnelle numérique, dont les compétences techniques, professionnelles et pédagogiques ont été rigoureusement évaluées et validées dans le cadre de nos procédures internes de sélection.
Cette formation est délivrée en partenariat avec notre partenaire *ACG Cyber Academy*

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement