MAÎTRISER LES RISQUES CYBER

Les enjeux de la cybersécurité ne cessent de prendre de l'ampleur en raison de l'accélération de l'évolution technologique. Les entreprises doivent maitriser à la fois des dimensions humaines et techniques pour conduire des projets de transformation digitale et respecter des nouvelles exigences réglementaires comme DORA et NIS2.
Cette formation va permettre de comprendre les fondamentaux des risques cyber et d'avoir un aperçu des acteurs et des menaces les plus courantes dans chaque composant du système d'information.

LES PLUS DE DE LA FORMATION

→ Une vulgarisation des concepts techniques qui deviennent accessibles aux généralistes des métiers du risque

→ Une approche complète pour appréhender à son rythme les concepts clefs des risques cyber à travers des modèles reconnus et des exercices pratiques tirés de l'expérience du formateur

→ Une compréhension des normes de la sécurité de l'information avec un benchmark des bonnes pratiques applicables à l'audit

1 JOUR/7h

8h45 - 17h30

Présentielle

Paris intra muros

Adhérents IFACI : **805 € HT**
Non adhérents : **960 € HT**

Déjeûner(s) inclus

CPE 7

16 participants

ref. Environment

2 DATES
- 16/05
- 11/12

4,6/5

Code formation : **25CYB**

Inscription inter : formation@ifaci.com
Information :
01 40 08 (48 08 / 47 85)
www.ifaci.com

Déclinaison de cette formation en INTRA selon vos spécificités : contactez-nous au **01 40 08 (48 05 ou 48 06)** ou **intra@ifaci.com**

PARTICIPANTS

Auditeurs internes, contrôleurs internes, responsables sécurité des systèmes d'information (RSSI), responsables du plan de continuité d'activités (RPCA), auditeurs IT.

Accessibilité - *cf. page 11*

PRÉREQUIS

Avoir suivi la formation "Désacraliser les systèmes d'information"

OBJECTIFS PÉDAGOGIQUES

→ **Acquérir** une culture des risques cyber à la fois organisationnelle et technique
→ **Découvrir** les principales normes de la cybersécurité (ISO27001, CIS20, OWASP).
→ **Identifier**, investiguer et évaluer les risques propres à la cybersécurité.
→ **Découvrir** les risques principaux liés au cyber de NIS2 (Network Information Security 2) et DORA (Digital Operational Resilience Act)

CONTENU

→ **Concepts et principes de la cybersécurité : DICT, Défense en profondeur, OPPT**
→ **Revue des typologies des cybercriminels avec quelques chiffres clés**
→ **Identification des menaces et vulnérabilités de chaque composant du système d'information :**
- Les risques de l'accès physique et les points de contrôles
- Les risques applicatifs avec OWASP Top10 avec des illustrations
- Les risques réseaux avec le modèle OSI (exemples d'attaques et de solutions)
- Les risques Infrastructure avec une illustration sur le Cloud computing
- Les mesures organisationnelles avec les différents acteurs de la cybersécurité

→ **Introduction aux principaux risques NIS2 et aux 5 piliers de DORA**

MOYENS PÉDAGOGIQUES

Visuels de présentation – fiches techniques – exercices – alternance de mises en application, de retours d'expériences et d'exposés, vidéos illustratives de l'ANSSI

MODALITÉS D'ÉVALUATION DES ACQUIS

Progression des apprentissages et évaluation des acquis des participants réalisés par le formateur tout au long de la formation (temps d'échanges, travaux pratiques, exercices d'entraînements, quiz...).

Une évaluation de la satisfaction de chaque stagiaire est réalisée en ligne. Cette évaluation est complétée par l'appréciation du formateur à l'issue de chaque session.

INTERVENANT

Un professionnel de l'audit interne et de la cybersécurité certifié CISM, CISA, CRISC, CDPSE, ISO27001 LA