1 jour (7 heures)
PRÉSENTIEL OU DISTANCIEL
▸ 05/10/2022

Adhérent
850 € HT

Non-adhérent
940 € HT

Public concerné
Trésoriers et banquiers utilisant SWIFT, responsables informatiques et interlocuteurs IT de trésorerie, auditeurs, consultants, responsables sécurité.

Prérequis
Aucun prérequis

Moyens pédagogiques et d'évaluation
- Études de cas
- Activités digitales
- Rapport d'auto-évaluation

LE CASH MANAGEMENT

PRÉPARER L'ÉVALUATION ANNUELLE SWIFT CSP

(CUSTOMER SECURITY PROGRAMME)

COMPÉTENCES VISÉES

- Comprendre les enjeux du Customer Security Programme de SWIFT
- Mieux connaître SWIFT et les différentes architectures de connexion au réseau
- Identifier le périmètre des contrôles de sécurité concernés par le programme
- Détailler la liste des contrôles de sécurité
- Se préparer et organiser l'évaluation des contrôles, remplir son attestation CSP

PROGRAMME

INTRODUCTION ET CONTEXTE DE LA MISE EN PLACE DU CSP

- Historique du programme et faits marquants
- Objectifs du CSP
- Panorama de la menace informatique et des étapes classiques d'une fraude
- Exemples de mesures de protection

LES ARCHITECTURES DE CONNEXION A SWIFT

- Services de messagerie et interfaces SWIFT
- Options de connexion à SWIFT (directe, via Service Bureau ou Alliance Lite2)
- Types d'architecture définis dans le CSP

LISTE DES CONTROLES ET DES MESURES DE SECURITE A METTRE EN PLACE

- Périmètre des mesures de sécurité
- Liste et détail des mesures de sécurité
- Risques couverts et options de mise en place des contrôles

EVALUATION INDEPENDANTE ET ATTESTATION ANNUELLE

- Cadre de l'évaluation indépendante
- Documentation mise à disposition par SWIFT
- Étapes de l'évaluation, acteurs impliqués et répartition des rôles et responsabilités
- Portail SWIFT (KYC-SA) pour soumettre son attestation et suivre le niveau de conformité de ses contreparties