

FRAUDE À L'ASSURANCE ET CYBER-RISQUES

Objectifs pédagogiques :

- Définir la fraude à l'assurance et la distinguer des notions voisines : erreur, fausse déclaration non intentionnelle, dol et faute dolosive
- Identifier les typologies et les modes opératoires de la fraude à la souscription, au sinistre et en interne
- Mettre en œuvre les dispositifs de détection et d'enquête dans le respect du RGPD et du régime des données d'infraction
- Mesurer les sanctions civiles et pénales encourues et articuler la lutte anti-fraude avec le dispositif LCB-FT
- Reconnaître les principales cyber-menaces et leur qualification pénale : atteintes aux systèmes de traitement automatisé de données, extorsion, atteintes aux traitements de données
- Maîtriser le cadre réglementaire cyber applicable à l'assurance : DORA, NIS 2, RGPD et AI Act
- Analyser les garanties, exclusions et conditions de souscription d'un contrat de cyber-assurance, y compris le dépôt de plainte sous 72 heures prévu à l'article L12-10-1 du Code des assurances
- Organiser la gestion de crise, la coopération avec les autorités et une gouvernance conjointe fraude et cyber

Public visé :

Intermédiaires en assurance (IAS), collaborateurs en cabinet, agents généraux, courtiers, conseillers clientèle, conseillers en gestion de patrimoine.

Prérequis :

Aucun. Des connaissances de base en assurance ou en gestion du risque sont un plus.

Durée :

15 heures

Modalité pédagogique :

Formation à distance (e-learning)

Méthodes pédagogiques :

Cours théoriques rédigés, quiz d'évaluation

Attestation :

Attestation de formation délivrée, conforme à l'obligation annuelle de formation continue des IAS

Conformité réglementaire :

Formation conforme à la Directive DDA (UE) 2016/97 et aux articles du Code des assurances relatifs aux IAS

Accessibilité :

Disponible 24h/24 sur tous supports (ordinateur, tablette, smartphone)

PROGRAMME DE FORMATION

Partie I – Fondamentaux juridiques de la fraude à l'assurance

Partie II-A – Typologies et modes opératoires de la fraude

Partie II-B – Détection, enquête, ALFA et RGPD

Partie III – Sanctions, LCB-FT et contentieux de la fraude

Partie IV – Cyber-menaces : typologie et répression pénale

Partie V – Cadre réglementaire cyber : DORA, NIS 2, RGPD, AI Act

Partie VI – Cyber-assurance et régime LOPMI des rançons

Partie VII – Gestion de crise, gouvernance conjointe et convergence fraude / cyber

Conclusion