# AML : Cybercriminalité - Détection des techniques de blanchiment dans la cybercriminalité

## OBJECTIFS

Bienvenue dans notre formation axée sur la lutte contre les pratiques de blanchiment et le financement du terrorisme, avec une attention particulière portée à la criminalité numérique. Dans un monde en constante évolution, il est essentiel de développer des stratégies efficaces pour relever les défis croissants du blanchiment et du financement du terrorisme. Cette formation soigneusement conçue vise à équiper les professionnels du secteur financier des connaissances et compétences nécessaires pour identifier, prévenir et combattre les activités de blanchiment d'argent.

La première partie de cette formation met en lumière les aspects clés du blanchiment d'argent, en fournissant une compréhension approfondie des mécanismes de fonctionnement, du processus lui-même et de l'application de la théorie des 3 phases, ainsi qu'une diversité de typologies de blanchiment (techniques). Le blanchiment est toujours alimenté par des activités illégales sous-jacentes, également appelées "délits sous-jacents". Dans ce contexte, une catégorie éminente est abordée : les crimes liés à la criminalité numérique, tels que le "hacking", le vol d'identité et la fraude informatique, ainsi qu'une référence à Internet en tant qu' "Iceberg" et une discussion du "Darknet". Une compréhension approfondie de la criminalité numérique contribue à l'identification de transactions inhabituelles, cruciales pour la détection du blanchiment et, dans certains cas, même pour le financement du terrorisme.

Les objectifs de cette formation sont les suivants :

- pouvoir situer les différentes typologies dans l'ensemble de la lutte contre le blanchiment (Crime Time Line – Ligne de temps du crime) ;
- pouvoir situer tous les acteurs dans les différentes étapes du processus de blanchiment de capitaux ;
- connaître et situer les typologies de blanchiment utilisées dans les différentes phases du processus de blanchiment ;
- acquérir une compréhension du déroulement du processus de blanchiment et de la combinaison de différentes typologies ;
- apprendre une attitude de "scepticisme professionnel" concernant les typologies de blanchiment ;
- acquérir une compréhension d'une autre catégorie de délits sous-jacents : la cybercriminalité.

## RESUME

Catégorie:

- Compliance & audit
- Gestion financière des entreprises

Niveau:

Avancé

Type de formation:

Formation en classe

Prix:

- Membre: € 550.00
- Non-membre: € 650.00
- Partner BZB: € 550.00
- Partner Cevora: € 475.00
- Incompany: sur mesure, prix à la demande

Heures de recyclage:

- Banque: **6h** général
- Assurances: **6h** général
- Crédits à la consommation: **6h** général
- Crédits hypothécaires: **6h** général
- Compliance: **6h**

## PUBLIC

---

La formation peut être suivie par différents groupes cibles :

- les responsables de la conformité - AMLCO (Anti-Money Laundering Compliance Officers) ;
- les employés des banques ;
- les employés des institutions d'assurance ;
- les employés en contact avec les fonds d'investissement (fonds, société de gestion, dépositaire, agent de transfert, distributeur) ;
- les employés en charge de la conformité ;
- les auditeurs internes ;
- les employés du département juridique ;
- les responsables de la lutte contre le blanchiment  dans les banques, les compagnies d'assurance, les fonds d'investissement ;
- les auditeurs et les contrôleurs internes ;
- les directeurs d'entreprise ;
- les responsables des départements juridiques et d'audit.

## CONNAISSANCE PRÉ-REQUIS

---

**Formation de niveau avancé :** cette formation requiert une connaissance générale de base du sujet.

## PROGRAMME

---

**CONTENU**

- Introduction
  - Objectif de la formation
  - Chronologie des crimes (Crime Time Line – ligne de temps du crime)
  - Qu'est-ce que le blanchiment ?
  - Pourquoi le blanchiment ?
  - Modèle de blanchiment : trois phases
  - Approche basée sur les risques (Risk-Based Approach, RBA) versus approche basée sur les typologies (Typology Based Approach, TBA)
  - Acteurs du blanchiment d'argent
  - Chaîne de signalement et d'enquête
  - Relation entre le blanchiment et le financement du terrorisme
  - Catégories de typologies de blanchiment d'argent
- Criminalité numérique
  - Qu'est-ce que la criminalité numérique?
  - Internet - "L'iceberg"
  - Darknet
  - Types de criminalité numérique
  - Criminalité financière versus criminalité numérique
  - Catégories de criminalité numérique
  - Criminalité numérique organisée
  - Fraude de type "Boiler Room"
  - Fraude du PDG ("CEO-fraude")
  - Fraude pyramidale

    - Fraude Ponzi
    - Fraude liée aux cryptomonnaies
    - Fraude aux options binaires
    - Criminalité numérique simple et semi-organisée
- Résumé - répétition

**INFORMATIONS PRATIQUES**

- **Durée :** 1 journée de formation (6 heures de formation)
- **Heures :** 09:00 à 17:00
- **Lieu:** Febelfin Academy : Phoenix building, Boulevard du Roi Albert II 19, 1210 Bruxelles

## MÉTHODOLOGIE

---

Une « **Formation en classe** » se suit en présentiel en groupe. Vous êtes présent avec les autres participants et le professeur à un moment convenu dans la même salle de cours. Il existe des possibilités d'interaction et de feed-back, tant des participants à l'enseignant qu'inversement. Le matériel didactique se compose comme base d'une présentation via la plateforme d'apprentissage MyFA, complétée de supports divers tels que syllabus numérique, présentation, extraits audiovisuels…

**Matériel didactique :** Présentation PowerPoint