Formation : Détecter les risques et les fraudes avec l'IA

Formation pratique - 2j - 14h00 - Réf. IUA
Prix : 2020 CHF H.T.

NEW

Cette formation permet de comprendre les mécanismes modernes de fraude et d'exploiter l'intelligence artificielle pour renforcer les dispositifs de surveillance. Les participants apprendront à détecter les anomalies, automatiser les contrôles et sécuriser les processus sensibles afin d'améliorer la prise de décision et la maîtrise des risques opérationnels.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Identifier les principales typologies de fraude et les zones de vulnérabilité dans les processus métiers.
- Analyser les signaux faibles et comportements atypiques afin de détecter les risques opérationnels.
- Exploiter des approches IA pour automatiser les contrôles et améliorer les dispositifs de surveillance.
- Sécuriser les processus sensibles en intégrant les enjeux réglementaires et les bonnes pratiques de gouvernance.

Public concerné

Responsables fraude, directions financières, auditeurs, contrôleurs internes, responsables conformité et toute personne impliquée dans la prévention des risques, les contrôles internes ou la sécurisation des processus opérationnels.

Prérequis

Aucun

Méthodes et moyens pédagogiques

Méthodes pédagogiques

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques, etc.

PARTICIPANTS

Responsables fraude, directions financières, auditeurs, contrôleurs internes, responsables conformité et toute personne impliquée dans la prévention des risques, les contrôles internes ou la sécurisation des processus opérationnels.

PRÉREQUIS

Aucun

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

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.

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.

Programme de la formation

1 Comprendre les mécanismes modernes de fraude

- Identifier les principales typologies de fraude financière, opérationnelle et documentaire.
- Analyser les comportements et méthodes utilisés par les fraudeurs dans les organisations.
- Cartographier les zones de vulnérabilité au sein des processus sensibles.
- Détecter les signaux faibles et indicateurs précurseurs d'incidents ou d'anomalies.

Travaux pratiques

analyse d'un scénario de fraude et cartographie des risques associés.

2 Renforcer les contrôles des processus opérationnels

- Contrôler les opérations de décaissement et sécuriser les paiements sensibles.
- Prévenir les fraudes fournisseurs et fiabiliser les processus d'achats.
- Sécuriser les processus RH, paie et gestion administrative des collaborateurs.
- Renforcer les contrôles liés aux notes de frais et aux justificatifs financiers.

Travaux pratiques

construction d'une grille de contrôle sur un processus métier sensible.

3 Exploiter l'intelligence artificielle pour améliorer la surveillance

- Comprendre les usages de l'IA dans la détection des anomalies et comportements atypiques.
- Déployer des approches prédictives pour identifier les risques de fraude.
- Automatiser les alertes, contrôles et mécanismes de surveillance opérationnelle.
- Accélérer les investigations grâce à l'analyse automatisée des données et événements.

Travaux pratiques

identification d'un cas d'usage IA applicable à un contexte métier.

4 Analyser les anomalies et accélérer les investigations

- Structurer une démarche d'analyse des alertes et incidents détectés.
- Prioriser les investigations selon le niveau de risque et l'impact métier.
- Exploiter les données disponibles pour consolider les éléments d'analyse.
- Formaliser les résultats d'investigation et les recommandations de sécurisation.

Etude de cas

étude de cas sur l'analyse d'anomalies et la priorisation des alertes.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

5 Encadrer les usages IA et sécuriser les données

- Comprendre les enjeux réglementaires liés à l'utilisation de l'intelligence artificielle.
- Garantir la fiabilité et la qualité des modèles utilisés dans les dispositifs de contrôle.
- Réduire les biais algorithmiques et renforcer la transparence des traitements.
- Sécuriser les données sensibles et encadrer les accès aux informations critiques.

Travaux pratiques
élaboration d'un plan de sécurisation et de gouvernance des usages IA.

6 Déployer une stratégie de prévention et de maîtrise des risques

- Structurer une démarche globale de prévention de la fraude et des risques opérationnels.
- Définir des indicateurs de suivi et des mécanismes de pilotage des contrôles.
- Sensibiliser les équipes aux bonnes pratiques de détection et de prévention.
- Construire un plan d'amélioration continue des dispositifs de surveillance.

Travaux pratiques
conception d'un plan d'action de prévention adapté à un environnement métier.

Dates et lieux

CLASSE À DISTANCE
2026 : 5 oct., 17 déc.