

Course : Detecting Risks and Fraud with AI

Practical course - 2d - 14h00 - Ref. IUA

Price : 1720 € E.T.

NEW

This training course provides an understanding of modern fraud mechanisms and teaches participants how to leverage artificial intelligence to strengthen monitoring systems. Participants will learn how to detect anomalies, automate controls, and secure sensitive processes in order to improve decision-making and manage operational risks.

Teaching objectives

At the end of the training, the participant will be able to:

- ✓ Identify the main types of fraud and areas of vulnerability in business processes.
- ✓ Analyze weak signals and atypical behaviors to detect operational risks.
- ✓ Leverage AI approaches to automate controls and improve monitoring systems.
- ✓ Secure sensitive processes by incorporating regulatory requirements and best practices in governance.

Intended audience

Fraud managers, finance departments, auditors, internal auditors, compliance officers, and anyone involved in risk prevention, internal controls, or ensuring the security of operational processes.

Prerequisites

None

Practical details

Teaching methods

The instructor assesses the participant's learning progress throughout the training course using multiple-choice questions, role-playing exercises, hands-on activities, and so on.

Course schedule

PARTICIPANTS

Fraud managers, finance departments, auditors, internal auditors, compliance officers, and anyone involved in risk prevention, internal controls, or ensuring the security of operational processes.

PREREQUISITES

None

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.

Participants also complete a placement test before and after the course to measure the skills they've developed.

1 Understanding Modern Fraud Schemes

- Identify the main types of financial, operational, and document-related fraud.
- Analyze the behaviors and methods used by fraudsters within organizations.
- Identify areas of vulnerability within sensitive processes.
- Detect weak signals and early warning indicators of incidents or anomalies.

Hands-on work

Analysis of a fraud scenario and mapping of the associated risks.

2 Strengthen controls over operational processes

- Monitor disbursement transactions and secure sensitive payments.
- Prevent supplier fraud and ensure the reliability of procurement processes.
- Secure HR, payroll, and administrative processes for employees.
- Strengthen controls related to expense reports and financial documentation.

Hands-on work

Development of a control framework for a sensitive business process.

3 Leveraging Artificial Intelligence to Improve Surveillance

- Understanding the uses of AI in detecting anomalies and atypical behavior.
- Implement predictive approaches to identify fraud risks.
- Automate alerts, checks, and operational monitoring mechanisms.
- Speed up investigations through automated data and event analysis.

Hands-on work

Identification of an AI use case applicable to a business context.

4 Analyze anomalies and expedite investigations

- Develop a process for analyzing detected alerts and incidents.
- Prioritize investigations based on risk level and business impact.
- Use the available data to strengthen the analysis.
- Document the findings of the investigation and the security recommendations.

Case study

Case study on anomaly analysis and alert prioritization.

5 Regulating AI Use and Securing Data

- Understanding the regulatory issues related to the use of artificial intelligence.
- Ensure the reliability and quality of the models used in control systems.
- Reduce algorithmic bias and enhance transparency in data processing.
- Secure sensitive data and control access to critical information.

Hands-on work

Development of a plan for the security and governance of AI applications.

TEACHING AIDS AND TECHNICAL RESOURCES

- The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
- At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
- A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

6 Implement a strategy for risk prevention and management

- Develop a comprehensive approach to preventing fraud and operational risks.
- Define monitoring indicators and mechanisms for managing controls.
- Raise awareness among teams about best practices for detection and prevention.
- Develop a plan for the continuous improvement of monitoring systems.

Hands-on work

Development of a prevention action plan tailored to a specific work environment.

This programme is an original creation, developed by the teaching teams at ORSYS Formation. Any reproduction, representation, adaptation or use, in whole or in part, without the prior written authorisation of ORSYS, is strictly prohibited. ORSYS reserves the right to take any action necessary to protect its intellectual property rights.

Dates and locations

REMOTE CLASS

2026 : 17 Dec.

2027 : 18 Jan., 24 May, 1 July, 26 Aug., 14 Oct.,
2 Dec.

BRUXELLES

2027 : 18 Jan., 24 May, 1 July, 14 Oct.

PARIS LA DÉFENSE

2026 : 10 Dec.

2027 : 18 Jan., 24 May, 1 July, 26 Aug., 14 Oct.,
2 Dec.

LUXEMBOURG

2027 : 18 Jan., 24 May, 1 July, 14 Oct.