AI in Fraud Detection and Proactive Risk Management Training Course



30 Nov - 04 Dec 2026

Cairo

3700 € (Per Person)

Ref: #AI7034_291188

Course Introduction / Overview:

In today's rapidly evolving digital landscape, financial institutions and corporations face an unprecedented surge in sophisticated fraud schemes and complex risks. Traditional rule-based systems are no longer sufficient to combat these dynamic threats. This course provides a comprehensive exploration of how Artificial Intelligence (AI) and Machine Learning (ML) are revolutionizing fraud detection and risk management. We will delve into the practical application of predictive analytics, anomaly detection, and deep learning to build resilient and proactive defense mechanisms. As discussed by author Agustín Rubini in his book "Artificial Intelligence in Finance", the integration of AI is not just an upgrade but a fundamental necessity for survival and growth in the modern financial ecosystem. This program, offered by BIG BEN Training Center, is meticulously designed to bridge the gap between theoretical knowledge and real-world implementation. Participants will learn to develop, deploy, and manage AI-driven systems that can identify suspicious activities in real-time, predict potential risks, and ensure regulatory compliance, thereby safeguarding organizational assets and reputation. This training course equips professionals with the critical skills to leverage AI as a strategic tool for creating a secure and intelligent operational environment.

Target Audience / This training course is suitable for:

- Fraud Analysts and Investigators.
- Risk Management Professionals.
- Compliance Officers and Managers.
- Data Scientists and Analysts working in finance.
- Internal and External Auditors.
- IT Security and Cybersecurity Specialists.
- Financial Controllers and Managers.
- Product Managers in FinTech and Banking.
- Executives and decision-makers overseeing risk and compliance functions.

Target Sectors and Industries:

- Banking and Financial Services.
- Insurance and InsurTech.
- Financial Technology (FinTech) and Payment Processors.
- E-commerce and Retail.
- Telecommunications.
- Healthcare and Medical Billing.
- Government, Regulatory Bodies, and Law Enforcement Agencies.
- Consulting and Professional Services.

Target Organizations Departments:

- Risk Management.
- Compliance and Anti-Money Laundering (AML).
- Internal Audit.
- Finance and Accounting.
- Information Technology (IT) and Cybersecurity.
- Data Analytics and Business Intelligence.
- Operations.
- Legal and Regulatory Affairs.

Course Offerings:

By the end of this course, the participants will have able to:

- Develop a strategic understanding of AI's role in modern fraud detection and risk management frameworks.
- Apply various machine learning algorithms to build effective fraud detection models.
- Utilize predictive analytics to proactively identify and mitigate financial and operational risks.
- Implement anomaly detection techniques to flag unusual patterns in large datasets.
- Understand the application of deep learning and neural networks for complex fraud scenarios.
- Design and evaluate AI-driven systems for regulatory compliance, including AML and KYC processes.
- Grasp the principles of Explainable AI (XAI) to ensure model transparency and accountability.
- Manage the lifecycle of AI models from development and deployment to ongoing monitoring.
- Formulate a robust AI governance strategy to address ethical and regulatory considerations.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, engaging, and practical, ensuring that participants can immediately apply their learning in a professional context. This course moves beyond traditional lectures to foster a dynamic learning environment built on a foundation of experiential learning. A significant portion of the program is dedicated to hands-on labs and workshops where participants will work with sample datasets to build and test their own machine learning models for fraud detection. We will analyze real-world case studies of sophisticated financial crimes and dissect the AI strategies used to uncover them. Collaborative group projects will encourage teamwork and problem-solving, simulating the cross-departmental efforts required to implement AI solutions effectively. Interactive sessions, expert-led discussions, and Q&A segments will provide ample opportunity for participants to engage with the instructor and peers, sharing insights and clarifying complex concepts. Continuous feedback and guided practice are integrated throughout the five days to reinforce learning and build confidence, ensuring a comprehensive mastery of the subject matter.

Course Agenda (Course Units):

Unit One: Foundations of AI in Fraud and Risk

- Introduction to Artificial Intelligence and Machine Learning.
- The Evolving Landscape of Financial Fraud and Cybercrime.
- Comparing Traditional Rule-Based Systems with AI-Powered Solutions.
- Key Concepts in Data Science for Fraud Detection.
- Data Preprocessing, Cleansing, and Feature Engineering.
- Ethical Considerations and Bias in AI Models.
- The Regulatory Environment and the Rise of RegTech.

Unit Two: Supervised and Unsupervised Machine Learning Models

- Understanding Supervised Learning for Fraud Classification.
- Logistic Regression and Decision Trees for Predictive Modeling.
- Support Vector Machines (SVM) and Random Forests.
- Introduction to Unsupervised Learning for Anomaly Detection.
- Clustering Algorithms (e.g., K-Means) to Identify Suspicious Groups.
- Principal Component Analysis (PCA) for Dimensionality Reduction.
- Building, Training, and Validating Your First Fraud Detection Model.

Unit Three: Advanced AI and Deep Learning Applications

- Introduction to Artificial Neural Networks (ANN).
- Applying Deep Learning for Complex and Subtle Fraud Patterns.
- Using Natural Language Processing (NLP) to Analyze Unstructured Data.
- Behavioral Analytics and Biometrics for Identity Verification.
- Detecting Synthetic Identity Fraud with Advanced AI.
- Graph Analytics and Network Analysis for Uncovering Fraud Rings.
- Generative Adversarial Networks (GANs) for Data Augmentation.

Unit Four: AI-Powered Risk Management Frameworks

- Applying AI in Credit Risk Scoring and Lending Decisions.
- Predictive Analytics for Operational and Market Risk Management.
- AI-driven Solutions for Anti-Money Laundering (AML) and Transaction Monitoring.
- Automating Know Your Customer (KYC) and Customer Due Diligence (CDD).
- Building Real-Time Risk Dashboards and Alerting Systems.
- Stress Testing and Scenario Analysis with AI Models.
- Integrating AI into the Enterprise-Wide Risk Management (ERM) Strategy.

Unit Five: Implementation, Governance, and Future Trends

- The Lifecycle of an AI Model from Deployment to Retirement (MLOps).
- The Importance of Explainable AI (XAI) for Stakeholders and Regulators.
- Techniques for Model Interpretability (SHAP and LIME).
- Developing a Robust AI Governance and Model Risk Management Framework.
- The Future of AI in Finance: Quantum Computing and Federated Learning.
- Addressing the Adversarial AI Threat.
- Capstone Project: Designing an End-to-End AI Fraud Detection System.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As AI models become more autonomous in fraud detection, how do we balance automated efficiency with the critical need for human oversight and ethical accountability?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by moving beyond purely technical instruction to cultivate a strategic, business-oriented mindset for leveraging AI in risk and fraud functions. While many programs focus solely on algorithms, our curriculum emphasizes the entire implementation lifecycle, from data preparation and model selection to deployment, governance, and crucially, Explainable AI (XAI). We dedicate significant time to ensuring participants can interpret and communicate model decisions to non-technical stakeholders, auditors, and regulators, a skill essential for real-world adoption and trust. The course content is uniquely structured to address both fraud detection and proactive risk management, providing a holistic view of how AI can be used not just to react to threats but to anticipate and mitigate them. Through a blend of hands-on labs using industry-relevant scenarios and deep dives into regulatory technology (RegTech) and ethical governance, participants gain a comprehensive and pragmatic skill set. This approach ensures graduates are not just data scientists but strategic leaders capable of building and managing resilient, intelligent, and compliant security frameworks.