Professional Certificate in AI in Financial Crime Compliance

Risk Assessment and Management in AI for Financial Crime Compliance

AI (Artificial Intelligence) refers to the simulation of human intelligence processes by machines, especially computer systems. These processes include learning (the acquisition of information and rules for using the information), reasoning (using the rules to reach approximate or definite conclusions), and self-correction.

AI in Financial Crime Compliance refers to the use of AI technologies, such as machine learning and natural language processing, to prevent, detect, and respond to financial crimes such as money laundering and terrorism financing.

Algorithmic Bias refers to the presence of systematic and repeatable errors in a machine learning model that result in unfair or discriminatory treatment of certain groups of people.

Anomaly Detection refers to the process of identifying unusual patterns or outliers in data that do not conform to expected behavior, which may indicate fraudulent or suspicious activity.

Anti-Money Laundering (AML) refers to a set of laws, regulations, and procedures designed to prevent, detect, and report money laundering and terrorism financing activities.

Churn Analysis refers to the process of analyzing customer behavior to identify and predict which customers are at risk of canceling a product or service.

Data Mining refers to the process of discovering patterns and knowledge from large amounts of data using AI, machine learning, and statistical methods.

Deep Learning refers to a subset of machine learning that involves the use of artificial neural networks with multiple layers to learn and represent data.

Explainability refers to the ability to understand and interpret the decisions made by an AI model, including the factors that contributed to the decision.

Feature Engineering refers to the process of selecting and transforming raw data features into meaningful variables that can be used to train a machine learning model.

Fraud Detection refers to the process of identifying and preventing fraudulent activities, such as credit card fraud, insurance claims fraud, and identity theft.

Generative Adversarial Networks (GANs) refers to a type of deep learning model that involves two neural networks, a generator and a discriminator, that are trained together to generate new data samples

that are similar to a given dataset.

Know Your Customer (KYC) refers to the process of identifying and verifying the identity of customers to prevent financial crimes such as money laundering and terrorism financing.

Machine Learning refers to a subset of AI that involves the use of algorithms and statistical models to enable machines to learn and improve from data without explicit programming.

Natural Language Processing (NLP) refers to the ability of machines to understand, interpret, and generate human language, including speech and text.

Neural Networks refers to a type of machine learning model inspired by the structure and function of the human brain, consisting of layers of interconnected nodes or neurons.

Risk Assessment refers to the process of evaluating the likelihood and impact of potential risks, including financial, operational, reputational, and compliance risks.

Risk Management refers to the process of identifying, assessing, and prioritizing risks, and developing strategies to mitigate or eliminate those risks.

Supervised Learning refers to a type of machine learning that involves training a model on labeled data, where the input data and corresponding output labels are provided.

Text Analytics refers to the process of extracting meaningful insights and patterns from text data using AI, machine learning, and statistical methods.

Transfer Learning refers to the process of using a pre-trained machine learning model as a starting point for training a new model, allowing the new model to benefit from the knowledge and experience of the pre-trained model.

Unsupervised Learning refers to a type of machine learning that involves training a model on unlabeled data, where the input data is not accompanied by corresponding output labels.

Virtual Currencies refers to digital or electronic currencies that are not issued or guaranteed by a central bank or government, and are not necessarily tied to a specific country or territory.

White Box Testing refers to the process of testing a machine learning model by examining its internal workings and decision-making processes, in order to identify and address any issues or biases.