XXVII
CONGRESO
HEMISFÉRICO
PANAMÁ 2023
16-17-18 DE AGOSTO

ASOCIACION BANCARIA
ABP
DE PANAMA

Audits of Artificial Intelligence systems used to monitor customer transactions and operations: a predictive analysis

Presented by:

Javier A. Almillátegui A., Director en Asesoría

Technology Enablement

Jason Chorlins, Principal, Financial Services Practice Leader

What's at Stake with Auditing AI?

- The stakes in managing data and technology are at an all-time high.
- Proper data and AI governance with an analogous innovation framework is critical to successful implementations.
- It remains critical to organizations to put controls in place to guarantee correct AI systems operations, focusing on preventing inappropriate/incomplete training data sets, privacy breaches, biased models, insecure/error prone models.
- Banks must prioritize the use of resources.
  - Critical processes need to be inventoried and then ranked in order of opportunity for automation/AI development and optimization.
- Data governance risk and process deficiencies may lead to informal or formal regulatory actions.
- Risk typically present for two reasons:
  1. fundamental errors which produce inaccurate outputs when compared to design objectives and intended use of a system or process; or
  2. incorrect or inappropriate use or misunderstood limitations or assumptions.

XXVII CONGRESO HEMISFÉRICO
PANAMÁ 2023

Do you speak Techlish?

- **Algorithm:** A step-by-step procedure for solving a problem of accomplishing some end, especially by a computer
- **Artificial Intelligence:** The development of computer systems able to perform tasks that normally require human intelligence
- **Machine Learning:** An application of artificial intelligence that provides systems the ability to automatically learn and improve without being explicitly programmed
- **Data Analytics:** The process of examining data sets in order to draw conclusions about the information they contain, increasingly with the aid of specialized systems and software

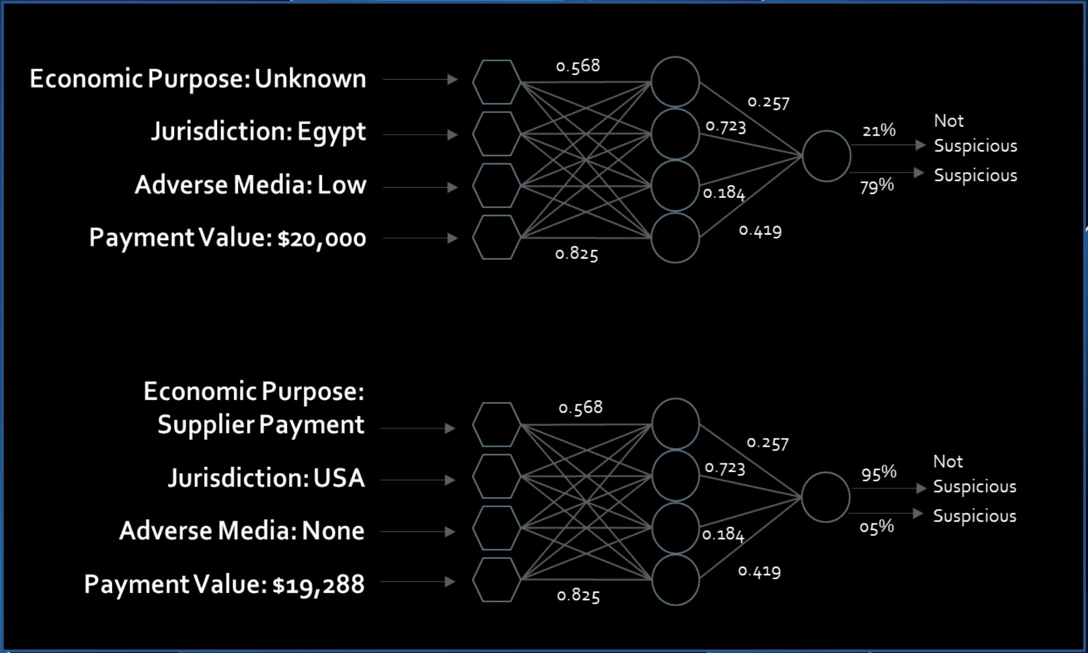
No One Way of Validating AI Techniques

AI techniques are as different as their applications - a variety of approaches will be required

- An Artificial Neural Network is a representation of a model that learns without **task-specific programming**

- Financial crime investigators **train** decision-making algorithms by presenting them with **red flags** and **suspicious activity**, alongside with the decision they would have made.

- Once trained, the neural network acts like a static model. Combinations of inputs result in output with a natural, measurable error rate.

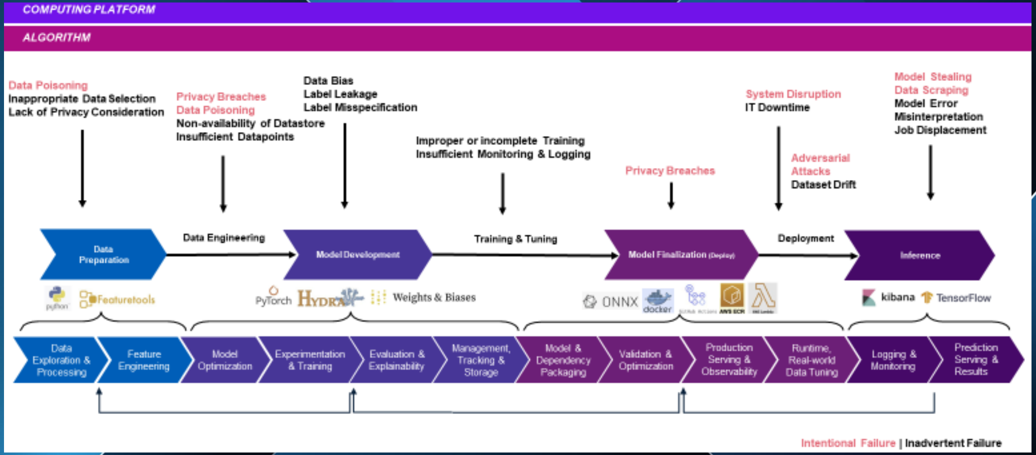


AI/ML development and operational Risks

Recent development Frameworks, such as KPMG Responsible AI Framework seek to put controls in place to handle AI Auditing needs:

- Development Controls
- Accountability of AI Usage.
- Transparency and Explainability of Decisions made by AI model
- Fairness of the model.

Also new tools have come to market, such as Mlflow, Dataiku, Cranium, etc… that enable easy adoption of MLOps.

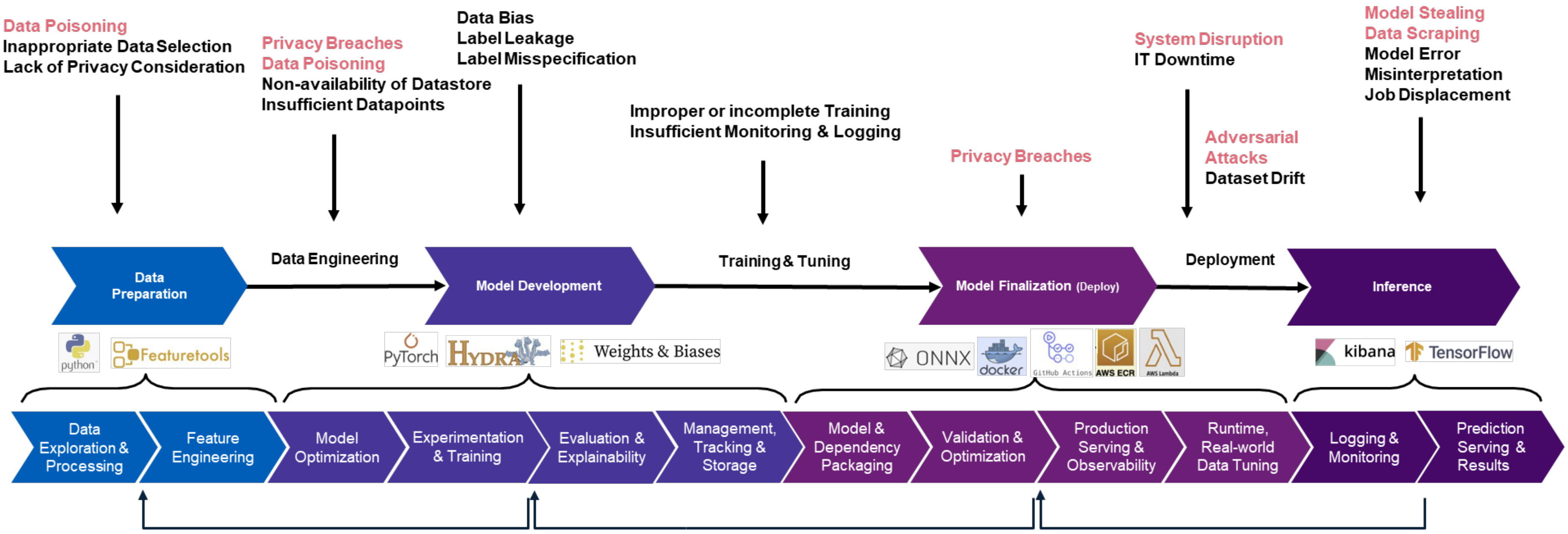


XXVII CONGRESO HEMISFÉRICO
PANAMÁ 2023

AI/ML Dev and Operational Risks

COMPUTING PLATFORM

ALGORITHM



Data Poisoning
Inappropriate Data Selection
Lack of Privacy Consideration

Privacy Breaches
Data Poisoning
Non-availability of Datastore
Insufficient Datapoints

Data Bias
Label Leakage
Label Misspecification

Improper or incomplete Training
Insufficient Monitoring & Logging

Privacy Breaches

System Disruption
IT Downtime

Adversarial Attacks
Dataset Drift

Model Stealing
Data Scraping
Model Error
Misinterpretation
Job Displacement

Data Preparation → Data Engineering → Model Development → Training & Tuning → Model Finalization (Deploy) → Deployment → Inference

Data Exploration & Processing
Feature Engineering
Model Optimization
Experimentation & Training
Evaluation & Explainability
Management, Tracking & Storage
Model & Dependency Packaging
Validation & Optimization
Production Serving & Observability
Runtime, Real-world Data Tuning
Logging & Monitoring
Prediction Serving & Results

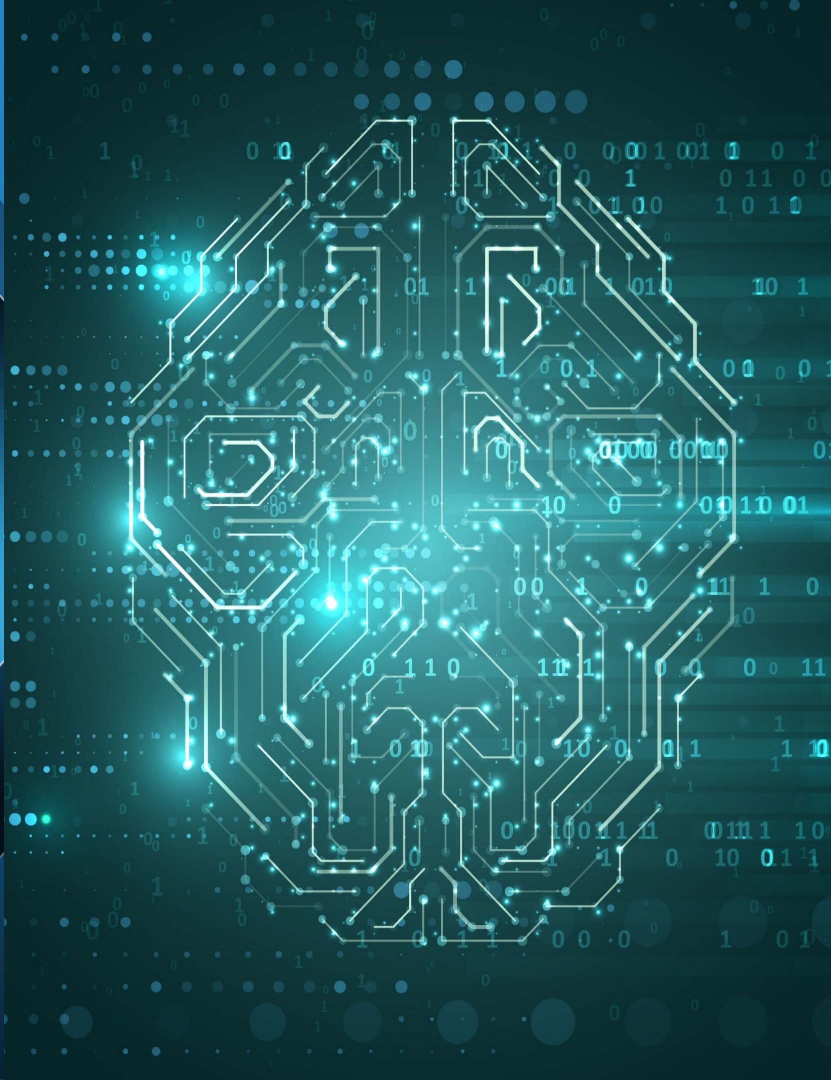
Intentional Failure | Inadvertent Failure

XXVII CONGRESO HEMISFÉRICO PANAMÁ 2023

How do you Evaluate Conceptual Soundness?

Evaluate the following factors:

- Data Integrity/Representativeness
- Bias
- Model Documentation/Explainability
- Parameter and Method Selection
- Training set curation



Challenges with Conceptual Soundness of AI Models

- Demonstrating the conceptual soundness of the models will be difficult if the math behind the ML/AI theory used to design them is not well understood and documented by the model developers, users and validators.

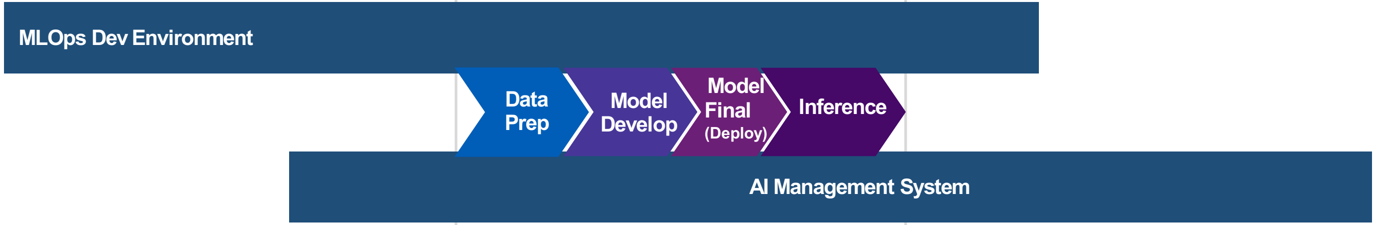
- ML/AI uses large volumes of structured and unstructured data, the dimensionality of the ML modeling features is much broader and deeper, making it challenging to ensure data integrity and representativeness.

- ML/AI models are difficult to explain and are often viewed as black boxes. Assessment of the variable selection process and explainability of driving factors become difficult due to the complexity and architecture of neural networks.

- MRM guidance requires that model documentation be comprehensive and detailed so that a knowledgeable third party can recreate the model without having access to the model development code.

AI/ML High Level Trust Ecosystem

DEVELOPMENT STACK


MLOps Dev Environment

Data Prep

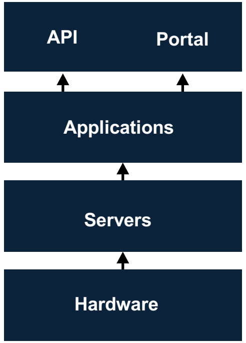
Model Develop

Model Final (Deploy)

Inference

AI Management System

DEV ENVIRONMENT STACK (CLOUD PLATFORM)


API

Portal

Applications

Servers

Hardware

ASSURANCE REPORTING

COMPUTING PLATFORM (SOC 2)

- Security
- Availability
- Data Confidentially
- Data Privacy

ALGORITHM ASSURANCE (SOC 2 Processing Integrity)

- Model Specifications and Processing
- Fair Model Treatments
- CI/CD w/ Continuous Training

GOVERNANCE (ISO 42001 AIMS)

- Fairness
- Accountability
- Transparency
- Explainability

Establishing Trustworthy AI

Key Takeaways

- Even if ML models perform better than traditional models, the lack of explainability may cause ML/AI models to be restricted in use by model validation and MRM teams.
- Future certification standards, such as ISO/IEC 42001 (Artificial Intelligence Management Systems) will allow for better governance of AI systems and the needs of the auditors.
- Document, Document, Document