# Empowering Operational Risks

## The Role of AI

*ABI*

13 June 2024



# Agenda

**Operational Risk Context**
Focus on Operational Risks

**ORM Management Process**
Focus on Operational Risk Management Process

**The future of Operational Risk Management**
Integration of AI

**AI: Practical Applications**
Use cases

Operational Risk Context

# Focus on Operational Risk

Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events


### Company Wide

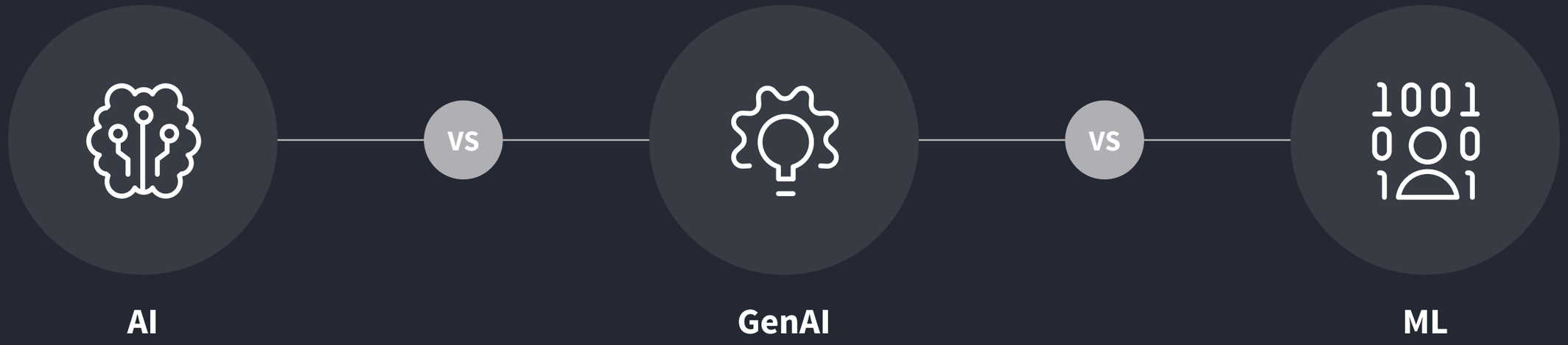
Risk management is a cross activity in a Company and a requirement in organizations of any dimension

### Constantly evolving

Complex organizational **structures** and new **business areas** require the management of risk and controls

Operational Risk Context

# AI vs GenAI vs Machine Learning



ORM Management Process

# Focus on the Operational Risk Management Process

## ORM Process

| Risk Identification | Risk Assessment | Risk Mitigation | Control Implementation | Risk Monitoring |
|---|---|---|---|---|
| Identify risks from various sources like internal processes, people, systems, and external events | Evaluate the identified risks to understand their nature and potential impact | Action plans that reduce the likelihood of the risk and/or the impact it would have if the risk were realized | Implement controls to reduce the likelihood or impact of risks. Establish procedures, policies, and safeguards to manage risks | Use key risk indicators (KRIs) and other metrics to track risk levels and detect changes. Regularly report risk status to stakeholders and senior management |

The Future of Operational Risk Management

# Integration of AI

## ORM Process & AI

| Risk Identification | Risk Assessment | Risk Mitigation | Control Implementation | Risk Monitoring |
|---|---|---|---|---|
| • Automate repetitive Tasks<br>• LDC Data Analysis<br>• Amplify Operational Risk Detection<br>• Automate Business Process Mapping and Risk Mapping | • Expert Judgement requested | • Identify Gap in controls and target effective mitigation strategies | • Expert Judgement requested | • Dynamic Risk Monitor<br>• Predictive Insights |

AI: Practical Applications

# Case I: Utilizing NLP for Loss Event Document Analysis

## Structured Data Extraction

- Extract named entities such as persons, places, organizations, loss amount, using NLP

## Describing and Summarizing Risk Events

- Summarize events by identifying the most important sentences or sections in the document

## Context

- Insert new LDC events
- Details from documentation
- The aim is to generate a summary with main information

## Auto-completion

- The A.I. automatically fills the fields required by the user interface with a suggestion for the ‘description’ of the event, the loss incurred, the BCBS class

# Case II: Utilizing AI for Business Process Modelling

## Context

- Details from process description documentation
- The aim is to generate a process flow chart with the main information

## AI – Drawing the Process

- AI automatically fills the fields required by the user interface with a suggestion of the process mapping comprehensive of controls, activities and by identifying the potential risks that can be mapped into the process

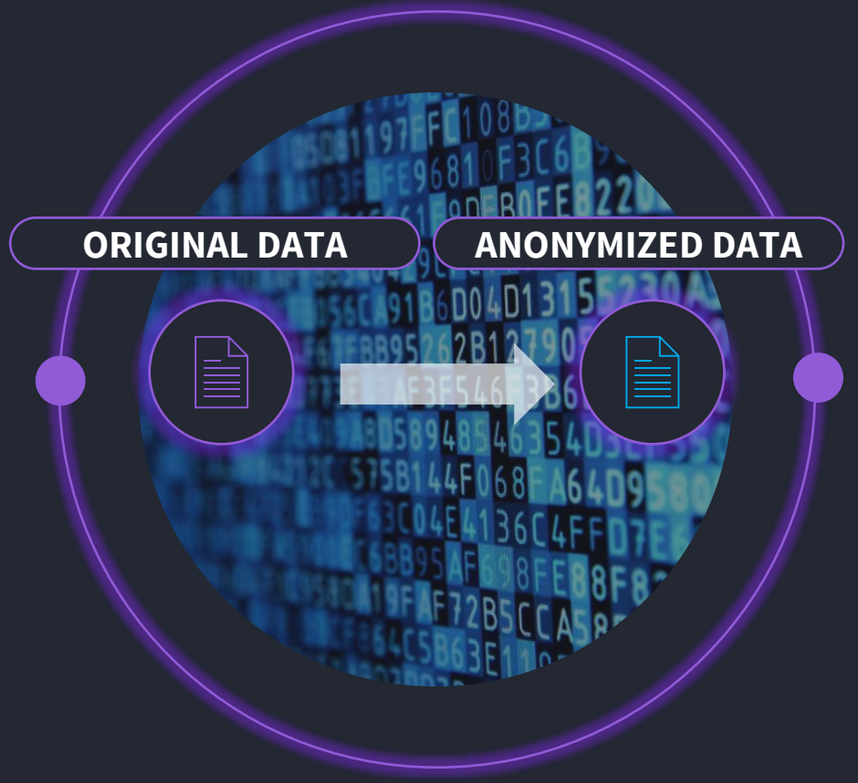
## Structured Data Extraction

- Extract named entities such as organizations involved, activities and controls performed

# Case III: Utilizing AI for Data Privacy Anonymization (GDPR)

## Context

- Collection of data from organization
- Strips data of elements that can link it to individuals or organizations:
  - Name
  - Other Variables
  - ID




## AI

- Data is anonymized and safe to share with other parties

# Case IV: Utilizing AI for AI Phishing Detection

## Context

- Fraudulent emails that appear to be from legitimate sources in an attempt to deceive recipients into revealing sensitive information, such as login credentials or financial details

## AI

- Advanced email AI phishing detection utilizes machine learning and NLP to analyze the content, context, and patterns of incoming emails:
  - URL Analysis
  - Contextual Analysis
  - Behavioural Analysis
  - Linguistic Analysis
  - Real Time Protection

*Don’t be afraid to fail. Be afraid not to try*

Michael Jordan


list