AI-enabled anti-money laundering

Discussion paper

Building a better working world

Table of contents

1. Introduction and overview

Financial crimes overview

- Financial crime is generally defined as any activity that involves fraudulent or criminal behavior for the purposes of personal financial gain.
- Financial crime ranges from basic theft or fraud committed by single individuals to large-scale, global schemes masterminded by organized criminal syndicates. Financial crime is commonly considered as covering the following offenses:

Different formats of financial crimes

Money laundering

Concealing the origins of illegally obtained funds through complex transactions to legitimize their source, the money is ultimately integrated to the legitimate economy.

Terrorist financing

Providing financial support to carry out acts of terrorism, often involving intricate networks to disguise the destination of funds.

Bribery and corruption

Exerting influence through offering or receiving value to gain an unfair business advantage or compromise integrity.

Fraud

Deceptive practices, such as false representation or manipulation, to gain an unfair advantage in financial transactions.

Insider trading

Illegally trading securities based on non-public information, often involving insiders with access to privileged data.

Cybercrime

Engaging in criminal activities using digital means, including fraud, hacking, and other cyber-related financial crimes.

■ Usually in-scope

▨ Sometimes in-scope

□ Rarely in-scope

The importance of financial crime risk management

Impact

Economy

Significant financial losses, reduced investor confidence, and increased costs for businesses

Social

Potential for inequality, loss of public trust, and compromised financial inclusion as vulnerable populations are disproportionately affected

Governance

Financial crime undermines the effectiveness of regulatory frameworks, erodes trust in institutions, and can lead to increased regulatory scrutiny

What is driving the need for financial crime risk management?

- Financial crime is considered one of the most impactful systematic risks in the global economy, with more than $2 trillion of illicit funds in circulation.
- It has a very important impact on society, resulting in a loss of integrity in financial systems, in economic and political stability, in the financing of terrorist activities and wars, and the threat to public health and social welfare.
- Risk management and the evolution of the treatment of financial crime is a critical part of safeguarding the stability of the financial sector.

Financial crime has reached new levels of sophistication using modern technologies.

The rapid development in information and financial technology allows you to move money anywhere in the world.

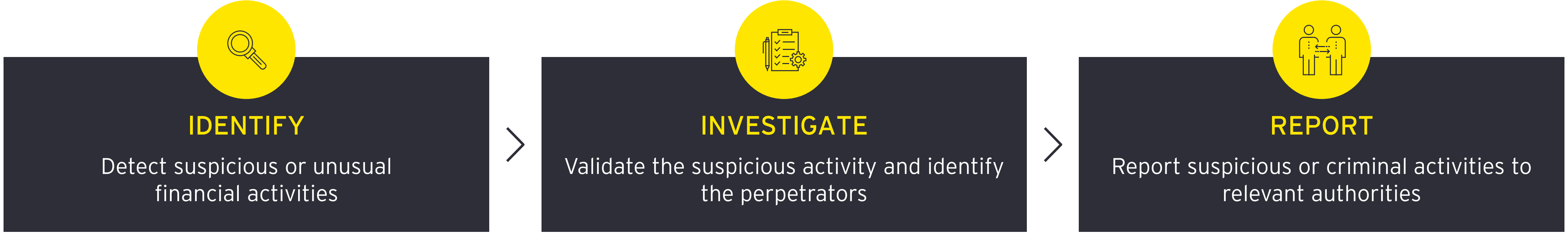
USD $342B[1] fines imposed by regulators globally since 2009	70% increase[2] in compliance costs since the financial crisis (2009)
USD $2.6B annual costs[2] from false alerts due to traditional compliance limitations	USD $2B illicit funds[3] in circulation

Institutions are moving away from physical advisor approaches to one based on technology and digital services to have more sustainable solutions.

1. U.S., EU fines on banks' misconduct to top $400 billion by 2020 - report | Reuters
2. How AI can address the increasing complexity of false positives in sanctions screening (pelican.ai)
3. What is Financial Crime? | Dow Jones

Common challenges in financial crime risk management

- Financial crime risk management in financial institutions typically consists of three key steps: **Identification, Investigation,** and **Reporting.**
- Despite best efforts, there are challenges in these process, which can **hinder compliance** to regulatory requirements, exposing the institution to **regulatory penalties**, and potentially **damage their reputation**.



IDENTIFY

Detect suspicious or unusual financial activities

INVESTIGATE

Validate the suspicious activity and identify the perpetrators

REPORT

Report suspicious or criminal activities to relevant authorities

CHALLENGES

- **Volume of transactions:** The sheer volume of financial transactions taking place daily can make it extremely challenging to detect suspicious activities.
- **False alerts:** Traditional systems may generate many false alarms, requiring resources to address.

- **Complex FinCrime schemes:** Criminals often use complex schemes of layered transactions to hide their activities.
- **Unstructured data analysis:** Investigating potential financial crimes often involves tedious, manual analysis of unstructured data to gain insights on relevant entities and individuals.

- **Quality of reports:** Reports need to be comprehensive and clear, which can be difficult and time-consuming to create.
- **Timeliness:** Delayed reporting can make it harder to catch criminals and prevent further crime.

How can AI help combat financial crimes?

AI technologies can offer compelling solutions in enhancing capabilities of detecting suspicious activities, streamlining the investigating processes, and improving reporting efficiency,

Identification: Emerging AI technologies can assist in managing vast transaction data sets efficiently and cutting down false positives by learning from historical patterns.

Use case examples: fraud detection, transaction monitoring, customer segmentation etc.

Investigation: AI technologies can introduce efficiency to the deep-dive investigation of suspect transactions, dismantling complex fraud schemes by recognizing patterns and gaining insights from complex unstructured data.

Use case examples: alert prioritization, AML investigation support etc.

Reporting: AI can help generate high-quality reports automatically, reducing manual work and the chance of errors, which ensures timely reporting of suspicious activities.

Use case examples: automated SAR generation etc.

These powerful capabilities enable higher efficiency and effectiveness in financial crime risk management, which could significantly improve the compliance to regulatory requirements

EFFICIENCY

AI automates routine tasks in financial crime risk management, enhancing timeliness in investigation and reporting processes, and boosting overall productivity

EFFECTIVENESS

AI enables timely and accurate recognition of criminal activities, reducing unnecessary works triggered by false alerts

COMPLIANCE

AI boosts financial crime identification and investigations ensuring organizations adhere to regulations and avoid penalties

2. AI-enabled anti-money laundering deep dive

AML overview and regulations

What is money laundering?

Money laundering is the processing of illegally obtained funds or assets through a series of transactions to conceal their true origin, ownership, and control in order to make those proceeds appear to have been derived from a legitimate source.

Why anti-money laundering is important?

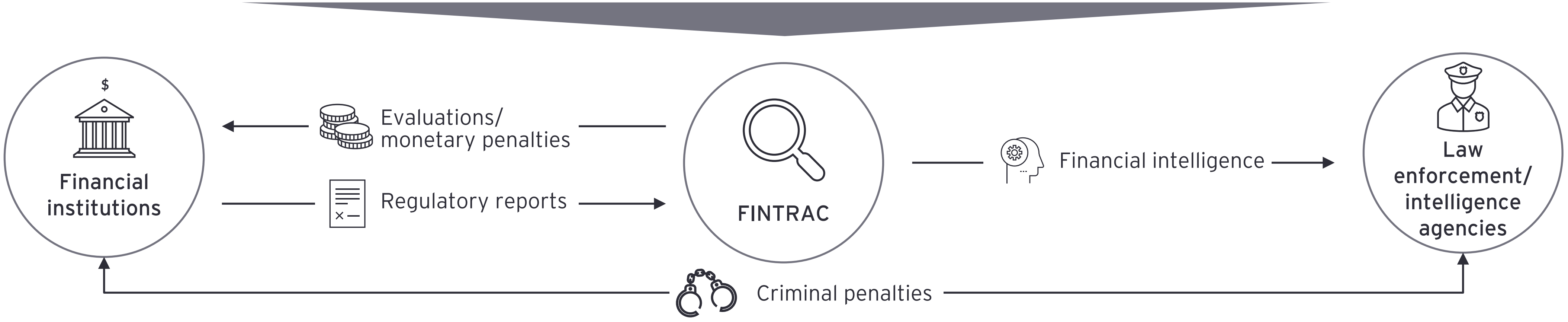
Money laundering would result in significant economic/social consequences (e.g., increased crime and corruption, economic distortion and instability, loss of tax revenue, etc.). Organizations that facilitate money laundering or terrorist financing, even if done inadvertently, are likely to face Regulator, Legal, Financial, and Reputational risks.

AML regulations in Canada

AML law:
AML is regulated by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)

AML vigilance:
The FINancial Transactions and Reports Analysis Centre of Canada (FINTRAC) is Canada's financial intelligence unit (FIU) that monitors compliance with the PCMLTFA.

AML intelligence:
FINTRAC interacts and cooperates with law enforcement and/or intelligence agencies including the Royal Canadian Mounted Police (RCMP), provincial/municipal police, and foreign FIU's.



How can EY help?

Current pain points

1

- Lack of accuracy causing unmanageable volume of false alerts
- New behavioural patterns not detected

2

- Lack of insights into complex behavioral fraud patterns e.g. smurfing, layering, circumvention

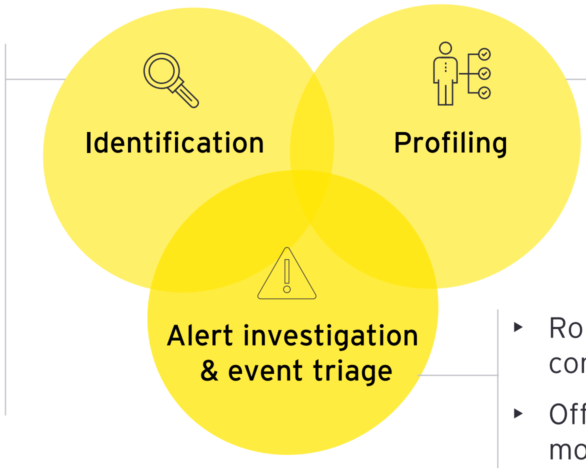
3

- Highly skilled compliance officers tackle false alerts
- Missing streamlined connected approach causes process inefficiencies

EY's approach

The EY organization has devised an anti-money laundering (AML) Solution aimed at helping optimize the accuracy of identifying suspicious clients and transactions, concurrently reducing operational expenses.

- Intelligently score each client /transaction and separates real cases from rest of the population
- Detects fraudulent patterns that are not known yet



- Profiles suspicious clients/transactions for enhanced root cause analysis
- Disclose main drivers of the model decision
- Derive rules explaining the model decision

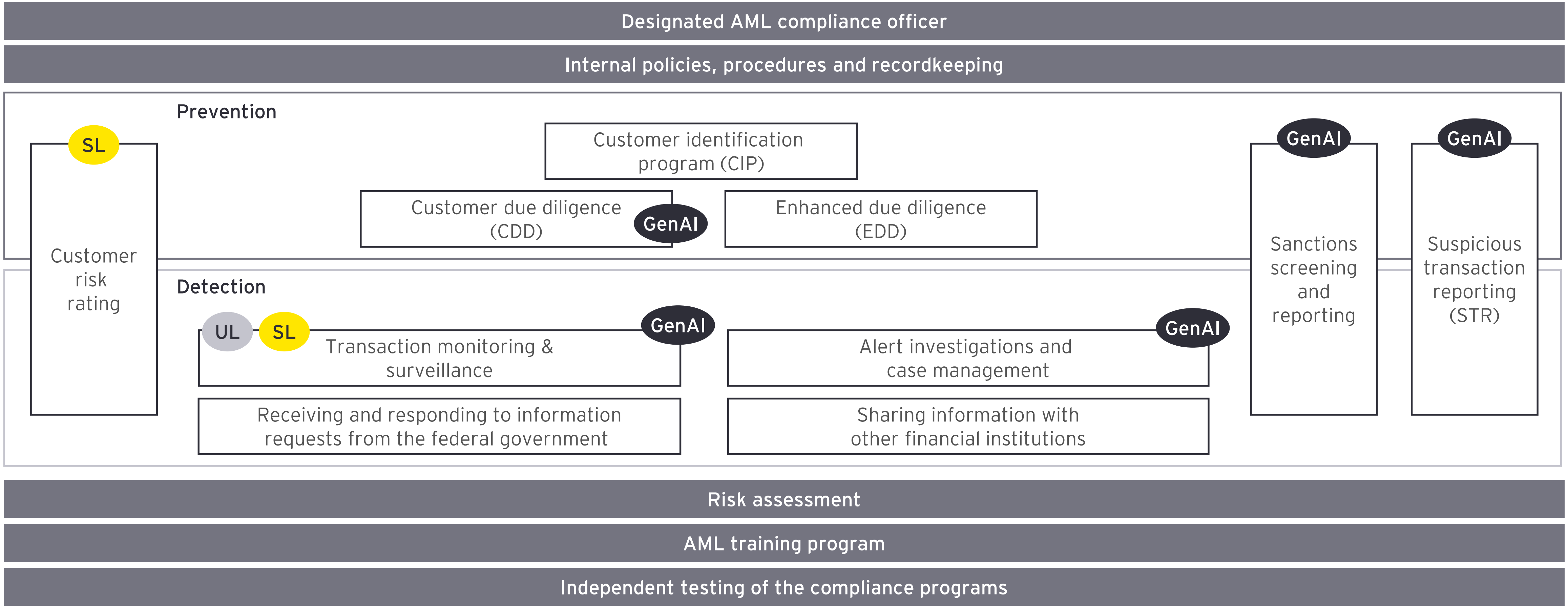
- Routes only complex investigations to highly skilled compliance officers
- Offers a broad solution supporting transaction/client monitoring as well as name screening actives

Benefits

- Reduction in false positive cases
- Operational savings in investigations and model management processes
- Efficient and effective monitoring
- Auditable and transparent process

AI for anti-money laundering (AML) overview

EY teams have extensive experience and capabilities for leveraging machine learning and natural language processing to help deliver solutions in the FinCrime space. Significant opportunity exist for utilizing generative AI (large language models) to add efficiencies and effectiveness throughout the AML lifecycle.



Designated AML compliance officer

Internal policies, procedures and recordkeeping

SL Customer risk rating

Prevention

- Customer identification program (CIP)
- Customer due diligence (CDD) GenAI
- Enhanced due diligence (EDD)

Detection

- UL SL Transaction monitoring & surveillance GenAI
- Alert investigations and case management GenAI
- Receiving and responding to information requests from the federal government
- Sharing information with other financial institutions

GenAI Sanctions screening and reporting

GenAI Suspicious transaction reporting (STR)

Risk assessment

AML training program

Independent testing of the compliance programs

Legend: UL Unsupervised learning SL Supervised learning GenAI Opportunity to apply generative AI

3. AI-enabled AML use case examples

Use case: transaction monitoring

Objectives

Current rule-based transaction monitoring system relies heavily on manual processes, resulting in a high number of false positives in the alert backlog for investigation. The EY organization aim to enhance the effectiveness and efficiency of the transaction monitoring by integrating advanced analytics models to reduce operating costs while simultaneously elevating detection quality, helping ensure regulatory compliance.

Approach

Preparation and data preprocessing

- Data preparation and querying
- Data profiling and exploratory analysis
- Data preprocessing
- Feature engineering based on our experience from previous projects

Model development and threshold tuning

- Unsupervised ML methods to perform clustering and identify suspicious cases
- Types of clustering algorithms:
  - Density based
  - Distance based
  - Distribution based
  - Depth based
  - Histogram based
- Derive thresholds from clustering models
- Robust sampling methodology for ATL/BTL testing
- Incorporate feedback from client SME to optimize model

Preparation of final results

- Incorporate qualitative review results from FIU and business insights to finalize model
- Prepare documentation and final reports

Benefits

- Calibrated thresholds based on robust modelling approaches reduce the false positive alerts and increase the efficiency of FIU investigation
- Rigorous testing and model validation process reduce the human errors and increase the model interpretability and replicability

Use case: ongoing monitoring for transaction monitoring models

The business case

Targeted business process

- The bank uses state-of-the-art Machine Learning models for its anti-money laundering transaction monitoring (TM).
- The governance of such models requires continuous monitoring of the input, output, and performance for each of these models.
- The current model monitoring framework needs to be strengthened and tested in the context of the integration of the portfolio acquisition.

Benefits

- Insights into the TM deviation model post-production based on the tests and analyses completed in the development of this pilot
- Proposed ongoing monitoring decision process for the pilot to support consistent decisioning based on diagnostics
- Ongoing monitoring framework for the pilot with insights on input drift, output drift and impact on performance

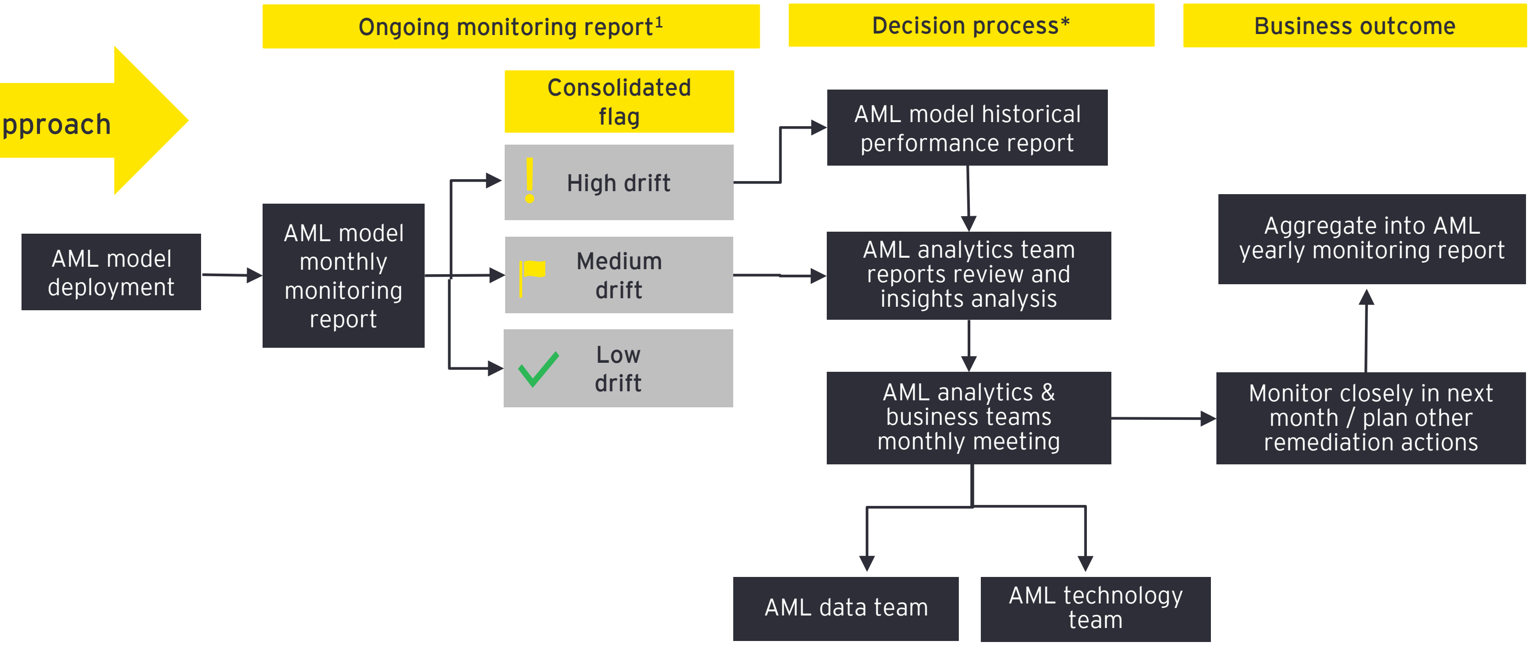
EY proposed solution

Objective

Develop an ongoing monitoring framework for the bank's TM deviation model for new accounts that:

- Supports the bank's business as usual (BAU) planning: insight into the customer portfolio, FIU alert volumes, risk through anticipated conversion rates, model maintenance, BAU below the line (BTL) testing strategy
- Can be leveraged in the portfolio acquisition integration

Approach


Ongoing monitoring report[1]
Decision process*
Business outcome
AML model deployment
AML model monthly monitoring report
Consolidated flag
! High drift
Medium drift
✓ Low drift
AML model historical performance report
AML analytics team reports review and insights analysis
AML analytics & business teams monthly meeting
AML data team
AML technology team
Monitor closely in next month / plan other remediation actions
Aggregate into AML yearly monitoring report

[1] The ongoing monitoring decision process can be calibrated based on business risk appetite and updated on an ongoing basis through active learning.

Use case: customer segmentation for transaction monitoring

The business case

Targeted business process

- Anti-Money Laundering laws and sophistication of criminal schemes pose challenges for financial institutions to quickly detect and report suspicious activities

Current pain points

- Existing segmentation practice applied to transaction monitoring based on simple expert judgement rules (using one or a limited number of business attributes) results in ineffective threshold setting, a large volume of false positives, and potentially false negatives
- High operational cost spent on the investigation of a high volume of false positive alerts, delayed investigation of (or potentially undetected) suspicious activities, difficulty to meet regulatory requirements

EY proposed solution

Objective

Enhance transaction monitoring efficiency by helping implement a customer segmentation strategy based on detailed customer profiles, such as KYC, account information, and risk ratings, along with transactional behavior analysis. This approach aims to reduce false positive alerts and operational costs, leading to increased productivity. Additionally, it serves to mitigate reputational and compliance risks.

Approach

- The approach includes three steps defined below:

Clustering

- Eliminate highly correlated features
- Help ensure feature consistency across transactional features
- Scale numerical features (e.g., minmax/standard scalar)
- Encode categorical features (e.g., one – hot encoding)
- Kmeans algorithm for customer segmentation
- Identify the best value of k through elbow method

Cluster interpretation

- Train an ensemble classification model (e.g., random forest) to predict derived cluster labels
- Shortlist top N features based on their feature importance scores
- Derive cluster profile based on top N important features

Threshold settings

- For threshold tuning, model - created clusters can be combined based on the qualitative feedback from business and below key factors:
- Similarity of data distribution (e.g., summary of statistics)
- Risk profile of each cluster
- Population size and transaction volume

Results & benefits

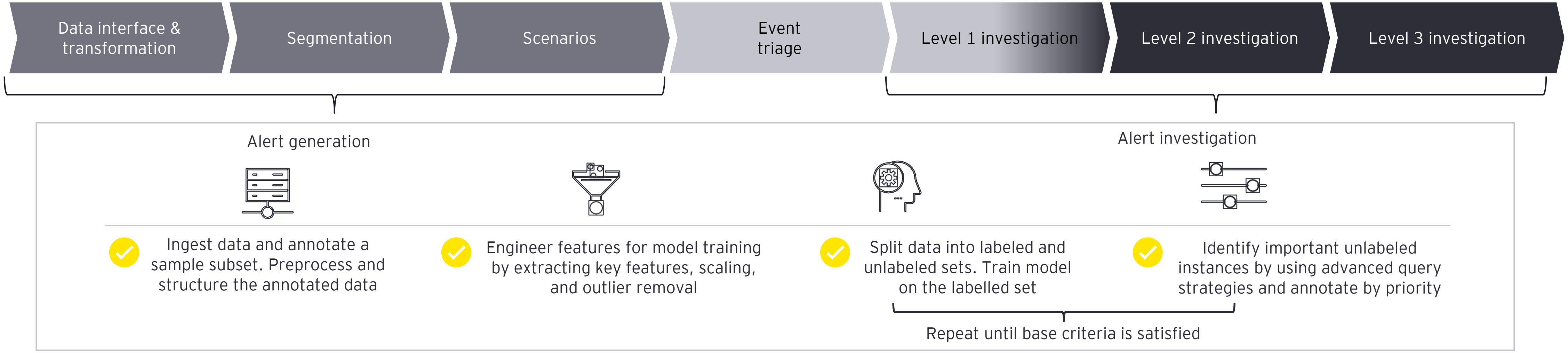
- Improve the efficiency and effectiveness of transaction monitoring using a customer segmentation based on more granular customer profile (e.g., KYC, account information, customer risk ratings) and transactional behaviour
- The EY organization was able to demonstrate a 55% reduction in false positives. Customer segmentation alone resulted in 20% reduction of false positives
- Reduce reputational and compliance risk

Use case: transaction monitoring alert prioritization

Objectives

Transaction monitoring models are largely based on unlabeled data as data labelling by investigators is costly and time-consuming. This poses a limitation to model performance improvement. Similarly, this results in alert backlogs. The objective is to be able to integrate Machine Learning techniques to prioritize labeling/investigation of the alerts.

Approach



- ✓ Ingest data and annotate a sample subset. Preprocess and structure the annotated data
- ✓ Engineer features for model training by extracting key features, scaling, and outlier removal
- ✓ Split data into labeled and unlabeled sets. Train model on the labelled set
- ✓ Identify important unlabeled instances by using advanced query strategies and annotate by priority

Repeat until base criteria is satisfied

Benefits

- Only a small number of labeled instances is required at the very first beginning, which is much smaller than the volume required for traditional supervised learning model
- It's an adaptive and incremental learning framework, which could greatly reduce the human labelling costs, have more flexibility to adapt to new risk patterns, and continuously improve the prediction accuracy.

Use case: AML investigation support with news insights

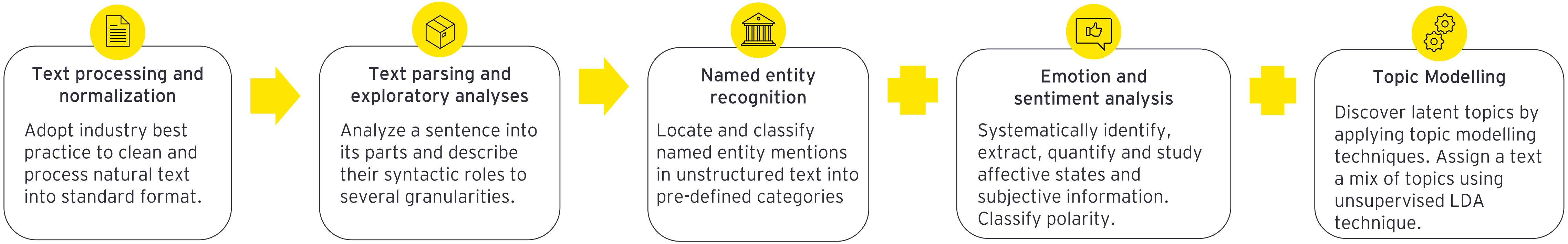
Objectives

Utilizing AI in AML investigation support involves extracting key individuals and locations from news articles, conducting sentiment analysis to characterize the polarity (positive, neutral, or negative), and summarizing the overall theme or topic of the news piece. This streamlined approach enhances the efficiency of news insight analysis for comprehensive AML investigations.

Approach

The EY organization aim to enhance the AML framework by incorporating news insight. Our strategy involves developing a natural language processing (NLP) model for news analysis with transparency and interpretability considerations.

News NLP process flow



Text processing and normalization

Adopt industry best practice to clean and process natural text into standard format.

Text parsing and exploratory analyses

Analyze a sentence into its parts and describe their syntactic roles to several granularities.

Named entity recognition

Locate and classify named entity mentions in unstructured text into pre-defined categories

Emotion and sentiment analysis

Systematically identify, extract, quantify and study affective states and subjective information. Classify polarity.

Topic Modelling

Discover latent topics by applying topic modelling techniques. Assign a text a mix of topics using unsupervised LDA technique.

Benefits

- Natural language processing (NLP) model for news analysis
- Comparison of different techniques and approaches
- Understanding of modeling assumptions and parameters
- Model outcomes, results, static visuals
- Transparency and interpretability considerations
- The improved detection rate expected to result in significant annual loss reduction.

Use case: generative AI for SAR generation

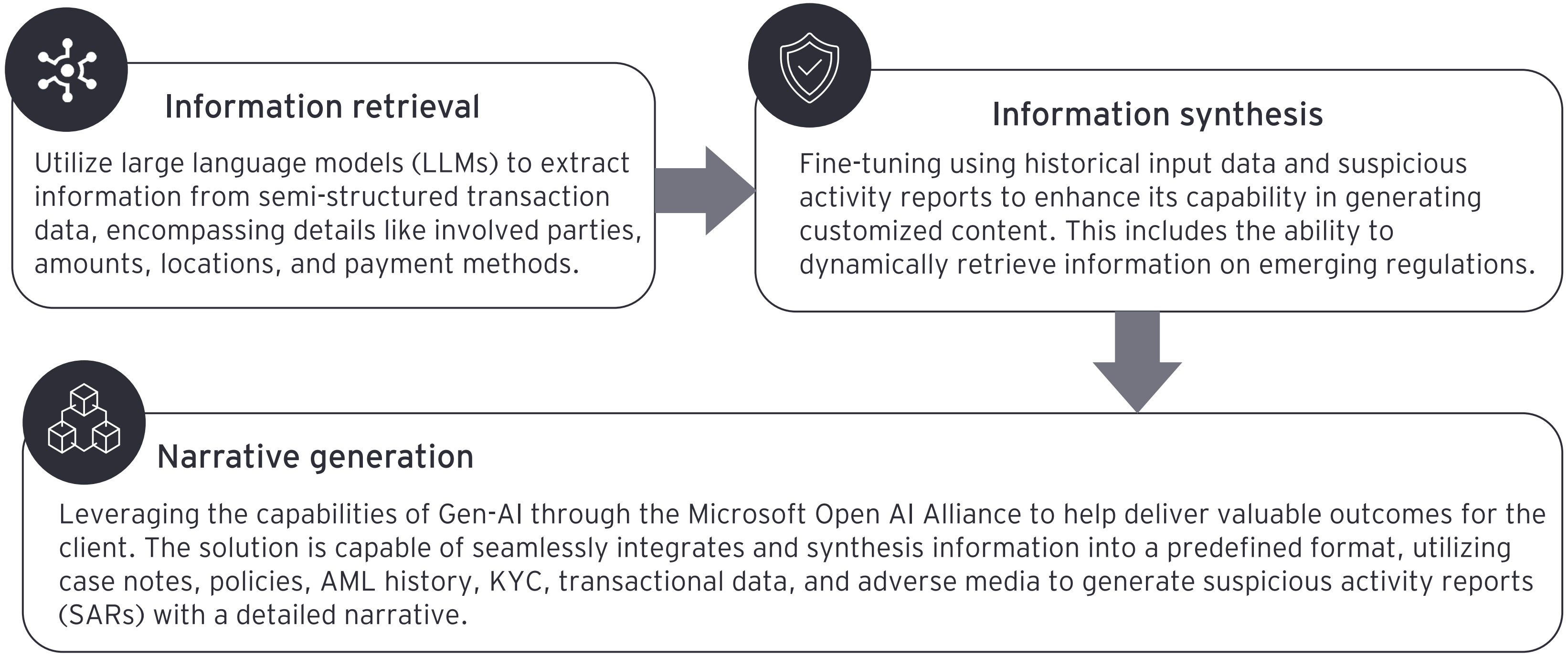
Objectives

The Gen-AI use case in the AML field aims to automate the generation of suspicious activity reports (SARs) with specific components.

This includes retrieving relevant facts on parties involved, detailing accounts and transactions chronologically, explaining the filer's position on the illegality or suspicion, and summarizing the report.

Gen-AI enables the generation of a comprehensive narrative, covering essential details like follow-up actions, names, locations, and additional information related to reported activities.

Approach



Information retrieval

Utilize large language models (LLMs) to extract information from semi-structured transaction data, encompassing details like involved parties, amounts, locations, and payment methods.

Information synthesis

Fine-tuning using historical input data and suspicious activity reports to enhance its capability in generating customized content. This includes the ability to dynamically retrieve information on emerging regulations.

Narrative generation

Leveraging the capabilities of Gen-AI through the Microsoft Open AI Alliance to help deliver valuable outcomes for the client. The solution is capable of seamlessly integrates and synthesis information into a predefined format, utilizing case notes, policies, AML history, KYC, transactional data, and adverse media to generate suspicious activity reports (SARs) with a detailed narrative.

Benefits

Helping implement automation in the SARs generation process will enhance efficiency, enabling a faster turnaround. Additionally, it ensures heightened consistency and adherence to both regulatory requirements and institutional guidelines.

Authors

Mario Schlener

Partner, Lead Financial Services Risk Management Practice and Enterprise Risk Strategy, EY Canada

EY Global FS Risk Technology, Alliance, Innovation Lead

mario.schlener@ca.ey.com

Ramzi Bou Hamdan

Associate Partner, Financial Crime and Anti-Money Laundering Lead, Financial Services Risk Management, EY Canada

ramzi.bou.hamdan@ey.com

Jean-Francois Isabelle

Executive Director, Practice Lead, FinCrime Innovation, EY Canada

Jean-Francois.Isabelle@ca.ey.com

Yara Elias, Ph.D.

Senior Manager, AI Risk Lead, Financial Services Risk Management, EY Canada

yara.elias@ca.ey.com

Hattie He, MSc.

Manager, AI and Data, Technology Consulting, EY Canada

Hattie.He@ca.ey.com

Liang Hu, Ph.D.

Manager, Responsible AI and AI Risk , Financial Service Risk Management, EY Canada

liang.Hu@ca.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

This publication contains information in summary form, current as of the date of publication, and is intended for general guidance only. It should not be regarded as comprehensive or a substitute for professional advice. Before taking any particular course of action, contact Ernst & Young or another professional advisor to discuss these matters in the context of your particular circumstances. We accept no responsibility for any loss or damage occasioned by your reliance on information contained in this publication.

ey.com/ca