



LEVERAGING AI TO TRANSFORM OPERATIONAL RISK MANAGEMENT (ORM) IN FINANCIAL SERVICES

Overview

Operational risk (OR) is the risk of loss stemming from deficient or failed internal processes and systems, or human errors and negligence, or due to external events. It is inherent in all activities, systems, products, and processes of an organization. OR includes risks such as cyber security risk, financial crime risk (money laundering, fraud, trade manipulation, etc.), technology and IT risk, vendor and outsourcing risks, business disruption risks, and many other types of risks. In several cases, financial institutions (FIs) also report legal and compliance risks under OR.

While organizations can make profits by accepting certain financial risks (like

market risks), OR only causes losses for organizations in the form of adverse impact to bottom line, reputational damage, etc. Resultantly, robust operational risk management (ORM) is a key focus area for all organizations including FIs.

Unfortunately, today many FIs' ORM systems are found wanting. These systems are unable to keep pace with the increasing business complexities. For example, these rigid rules-based systems lack capability to process unstructured data (text, voice, charts, etc.) and to offer real-time and actionable insights on the firm's OR.

Artificial intelligence and machine learning (AI/ML)-based solutions can address many of the shortcomings that are prevalent in the traditional ORM systems. AI/ML-based solution possess deep learning, robotic process automation (RPA), natural language processing (NLP), natural language generation (NLG), natural language understanding (NLU), image recognition, graph analytics, and other advanced capabilities. They leverage sophisticated supervised (example, KNN, LDA, QDA, ANN, OCSVM, LASSO, Naïve Bayes) and unsupervised (example, X-means, GMM, Bisecting K-means, AHMMAS) ML techniques. These systems can:

Perform high-speed processing of massive volume of data — both structured and unstructured — from wide array of sources to offer actionable insights
Enable automated data visualization
Automate repetitive tasks
Self-learn and adapt to changing scenarios
Offer accurate predictive capabilities — ML algorithm can effectively take into consideration numerous levels of non-linearity, high number of variables, and large data volume

AI and ML Use Cases for ORM in Financial Services


There is increasing adoption of AI and ML for ORM in financial services. Refer below few use cases.



Figure 1: Examples of AI/ ML Use Cases for ORM in Financial Services


OR Measurement and Monitoring

AI/ML-based solution can, for example, support:

	Modeling and measurement of OR for capital calculation, risk prioritization, risk decisioning, etc. — by applying Bayesian Networks and other sophisticated capabilities
	Forecasting of capital reserve required for OR
	Optimization of regulatory capital for OR
	OR quantification and scoring — by leveraging vast array of structured and unstructured data including historical OR loss data, incident database, internal risk indicators, control libraries, external loss data, risk reports, phone and messaging conversations, emails, adverse media/ negative news, and more
	OR self-assessment and development of key OR indicators
	Classification and aggregation of OR
	Enablement of early warning signals for various OR
	Improvements in existing OR controls
	Identification of idiosyncratic OR events — using isolation forest model, etc. to unearth events unlikely to recur
	Near real-time monitoring of OR
	Identify emerging OR — by parsing through myriad public data sources


OR Data Process Improvements

AI/ML-based solution can, for example, support:

	Enablement of robust operational data control — vis-à-vis research, reconciliation, remediation, and reporting
	Data augmentation — for example, analysis of free-text descriptions of loss events, NLP tagging of losses, interpolation of missing data, inferring missing attributes in control libraries based upon free text descriptions of control, etc.
	Automatic data categorization — example, using unstructured free-text descriptions to classify loss data
	Data quality assurance — through automatic identification of duplicated entries, data gaps/ inconsistencies, “fat-finger” errors, etc.
	Automation of repetitive and time-intensive data tasks — such as collection, handling, and analysis of OR data through RPA


OR Reporting

AI/ML-based solution can, for example, support:

	Sophisticated ORM reports and dashboards
	Automated analysis of disclosure (example, U.S. Securities and Exchange Commission (SEC) filings) to unearth risks in filings
	Reporting workflow automation


Model Risk Management

AI/ML-based solution can, for example, support:

	OR models optimization
	OR models validation and backtesting
	Modeling of uncertainty in operational risk — by leveraging probabilistic graphical models (PGM)


OR Stress Testing

AI/ML-based solution can, for example, support:

	Scenario analysis for OR stress testing (example, Dodd-Frank Act Stress Testing (DFAST), Comprehensive Capital Analysis and Review (CCAR))
	Optimization of scenarios for OR stress testing
	Automation of stress testing workflow
	Feature extraction for models utilized in OR stress testing — ML algorithms can process massive volumes of data to extract large number of relevant features
	Preparation of stress testing results and reports
	Automated analysis by regulators (example, SEC) of FIs' stress test reports — to identify anomalies


Third-party Risk Management (TPRM)

AI/ML-based solution can, for example, support:

	Enablement of 360° contextual awareness of the firm's third-party relationships and risks
	Sophisticated risk qualification and quantification — using current and historical risk exposure data (both structured and unstructured) on the third party
	Identification and prioritization of third-party risks
	Automatic mapping of third-party risks to associated controls, line of business (LOB), and stakeholders
	Management of third-party cyber risks
	Intelligent contract management with third-party
	Sophisticated reports and dashboards — on concentration risk, vendors risk score, service-level agreement (SLA) compliance, etc.
	Automated workflow and tools — for example, intelligent third-party risk assessment tools, sophisticated alerts, advanced alert routing and escalation to concerned teams


Compliance and Audit Management

AI/ML-based solution can, for example, support:

	Automated impact analysis of new/evolving regulations — by evaluating and interpreting massive volume of documents and sources on federal, state, and international regulatory guidelines
	Mapping of relevant regulations — using ML, NLP, RPA, etc. — to the concerned LOBs, products, systems, controls, processes, etc.
	Audit processes — for example, a) run semantic intelligence analysis to discover audit issues; b) enable moving away from the existing auditing methodology that are based on backward-looking sampling, onto a more continuous and comprehensive monitoring; c) automatically reading through, say over 500-page contract, to ascertain if there are any legal issues
	Robo-advisers, virtual assistants, and chatbots for internal compliance management and audit teams
	Real-time non-compliance alerts


Conduct Risk Management

AI/ML-based solution can, for example, support:

	Real-time behavioral analysis of staff — to unearth anomalies
	Automated analysis of staff related data — such as e-mails, instant messaging, documents, calendar items, phone calls, activity logs, building entry/exit time, etc. — for conduct risk identification
	Proactive identification of misconduct by market participants — for example, misleading marketing by unlicensed accountants that are engaged in providing financial advice

Cybersecurity Risk Management

AI/ML-based solution can, for example, support:

	Cyber risk scoring/quantification and residual-risk calculation
	Malware detection, analysis, and prevention
	Phishing and spam-detection and filtering
	Identifying the domain names generated by domain-generated-algorithms (DGAs)
	Cyber threat hunting
	Pentesting
	Network intrusion detection and prevention
	Thwarting advanced, persistent threats (APTs)
	Prevention of the zero-day attacks
	Automation of cybersecurity controls
	AI-based antivirus software
	Alert investigation and qualification
	False positives optimization
	Case review optimization (through document digitalization)

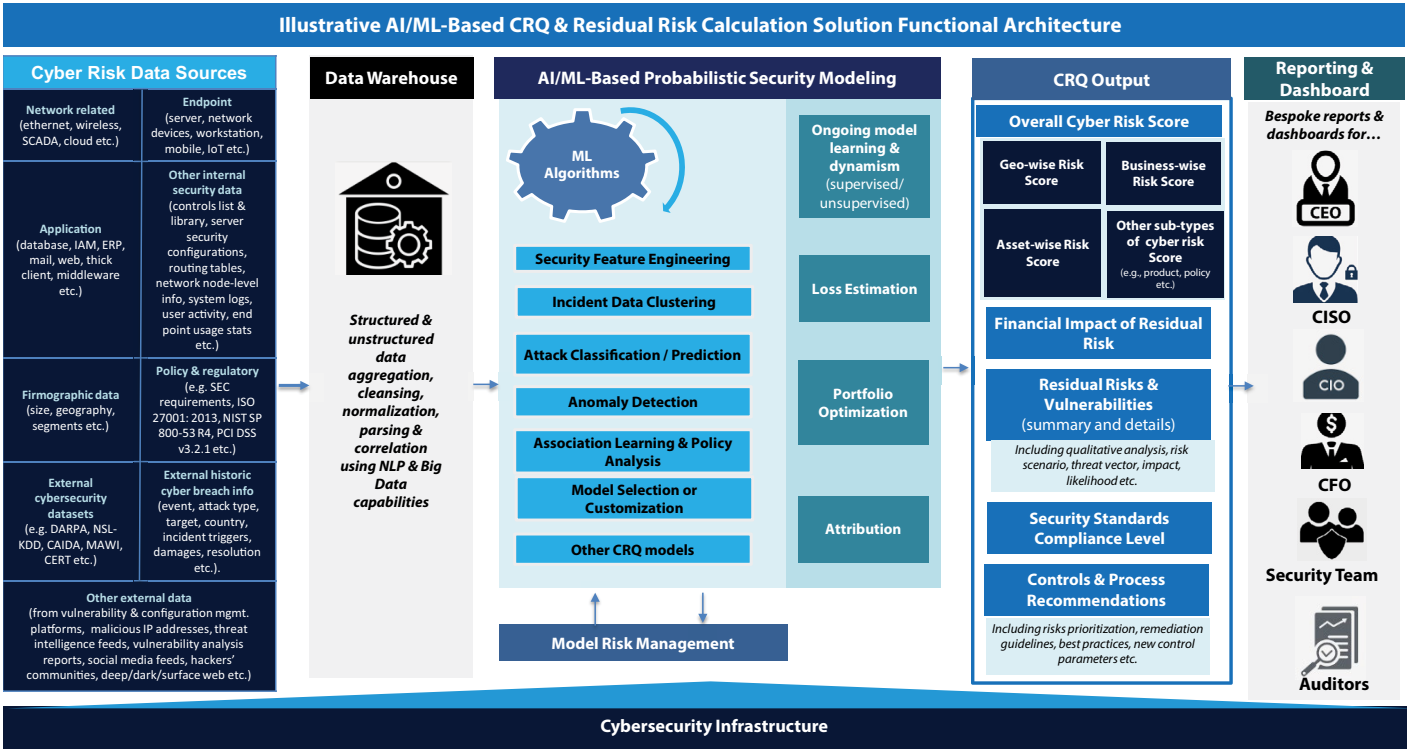




Figure 2: Illustrative AI/ML-Based Cyber Risk Quantification (CRQ) and Residual Risk Calculation Solution Functional Architecture


Financial Crime Risk Management (FCRM)

AI/ML-based solution can, for example, support:

Overall	
	Adaptive, real-time, and risk-based transaction monitoring
	Transaction screening — to detect potential instances financial crime
	Sophisticated risk scoring — to aid in prioritization of investigation queues for suspicious activity reporting (SARs)
	Customer onboarding and risk assessment (know your customer (KYC), customer due diligence (CDD), enhanced due diligence (EDD)). For example: a) real-time transaction-based KYC anomaly detection; b) dynamic questionnaire for customer onboarding; c) intelligent customer segmentation for KYC profiling; d) identity and background pre-checks for remote KYC
	Unearthing of financial crime and collusion by own by employees — by tracking in real-time employees' digital activities and communications (emails, chat etc.), and multiple other system parameters
	Detection of new financial crime scenarios
	Alert and case management — for example, a) alert tuning; b) alert triage and prioritization; c) alert routing; d) alert hibernation and risk-rating of alert groupings; e) false positive reduction; f) auto-suppression/closure of low-risk alerts; g) risk-based alert scoring and prioritization; h) intelligent alert routing; i) sophisticated case management; etc.
	Reporting and dashboards — for example, a) graphical, intuitive, and interactive visualization (of alerts, cases, etc.); b) intelligent reports and dashboards; c) support suspicious activity report (SAR), suspicious transaction report (STR), and suspicious transaction and order report (STOR), etc. submission
	Workflow automation — such as data processes; case management workflow; reporting workflow; customer onboarding; etc.

Anti-Money Laundering (AML)	
	AML screening — name screening; adverse media screening; sanctions and watchlists screening
	AML profiling and segmentation — intelligent profiling and segmentation; transaction threshold tuning
	Sophisticated link analysis — offering visual network maps (of relationships between entities including people, firms, suppliers, business partners, transactions, etc.)
	Specific AML risks intelligence — geographic, temporal, emerging, etc
	Ultimate beneficial owner (UBO) identification

Fraud Management	
	Real-time fraud detection via various banking channels — online, mobile, ATM, etc. — using logistic regression, neural network, and other advanced techniques
	Card and payment fraud detection — using artificial neural networks (ANNs), fuzzy system, support vector machines (SVM), genetic algorithm (GA), hidden Markov model (HMM), and other advanced capabilities
	Unearth formjacking of payment card detail
	Fake account identification
	Identity theft detection — by discovering inconsistencies in ID documents, etc.
	Detect loan application fraud
	Discover account takeover (ATO) attacks
	Identify chargeback fraud
	Detect insurance claims frauds (fake claims, duplicate claims, etc.)
	Locate absconding fraudsters — by searching public search engines, deep web, dark web, and available public databases to locate the whereabouts of absconding fraudsters and the banks that may be assisting them to move funds internationally

Trade and Market Surveillance	
	Communication surveillance — by enabling a) integrated communication surveillance; b) contextualization of communication; c) deciphering of jargons and code words; d) intelligent speech-to-text transcription; e) sophisticated communication storage; and f) multilingual communication surveillance
	Holistic surveillance — by enabling a) real-time data processing; b) smart segmentation; c) comprehensive, dynamic, and risk-based surveillance; and d) cross-asset class and cross-market surveillance
	Employee and trader surveillance — identify rogue traders, mis-selling by adviser, and the collusive manipulations (such as insider trading, benchmark rigging, etc.)
	Unearth novel and complex trade manipulations — including various forms of spoofing (including layering, vacuuming, collapsing of layers, flipping, spread squeeze, etc.); algorithmic trading (AT) and high-frequency trading (HFT) manipulations; and front running
	AML and trade surveillance integration
	Support enforcement by supervisory agencies — example, U.S. Consolidated Audit Trail (CAT) requirements; trade construction requirement; Regulation Best Interest (BI) and sales practices and suitability obligations; SEC filings (8-K) compliance
	Regulatory change implementation — for example, machine-readable rulebook, deciphering of new regulatory changes, support new regulatory change implementation; etc.

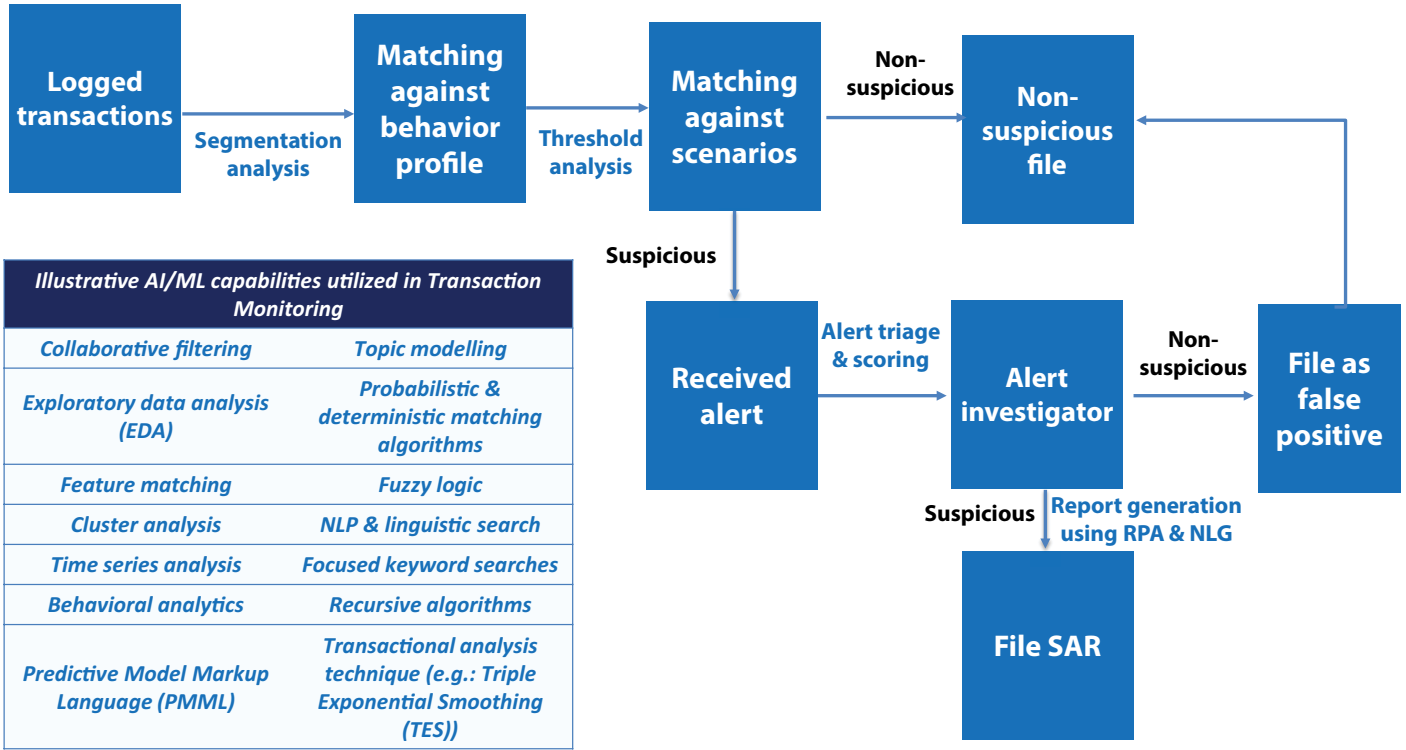


Figure 3: Illustrative AI/ML Role During Transaction Monitoring and Beyond

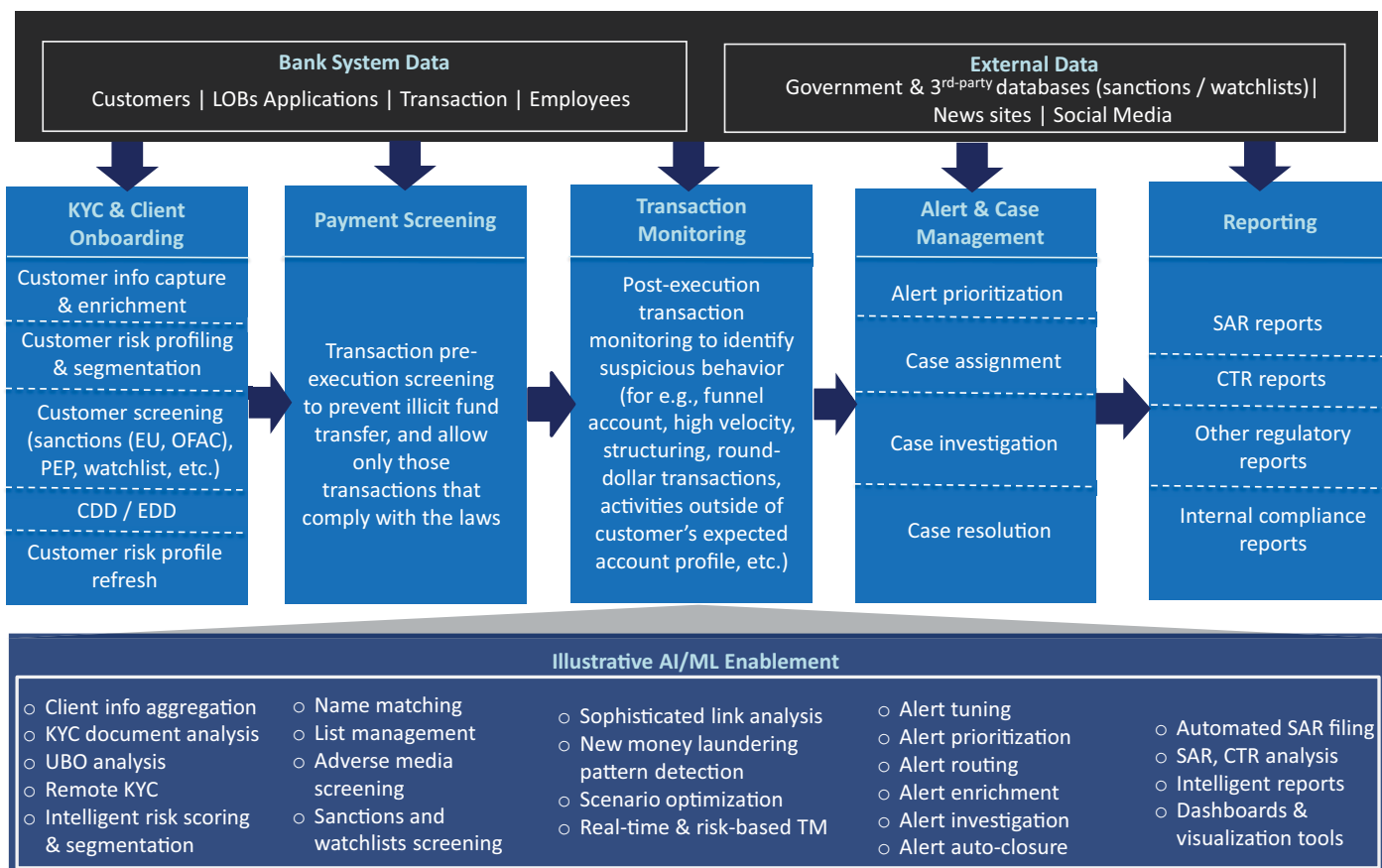


Figure 4: High-Level KYC-AML Workflow and Associated AI/ML Enablement

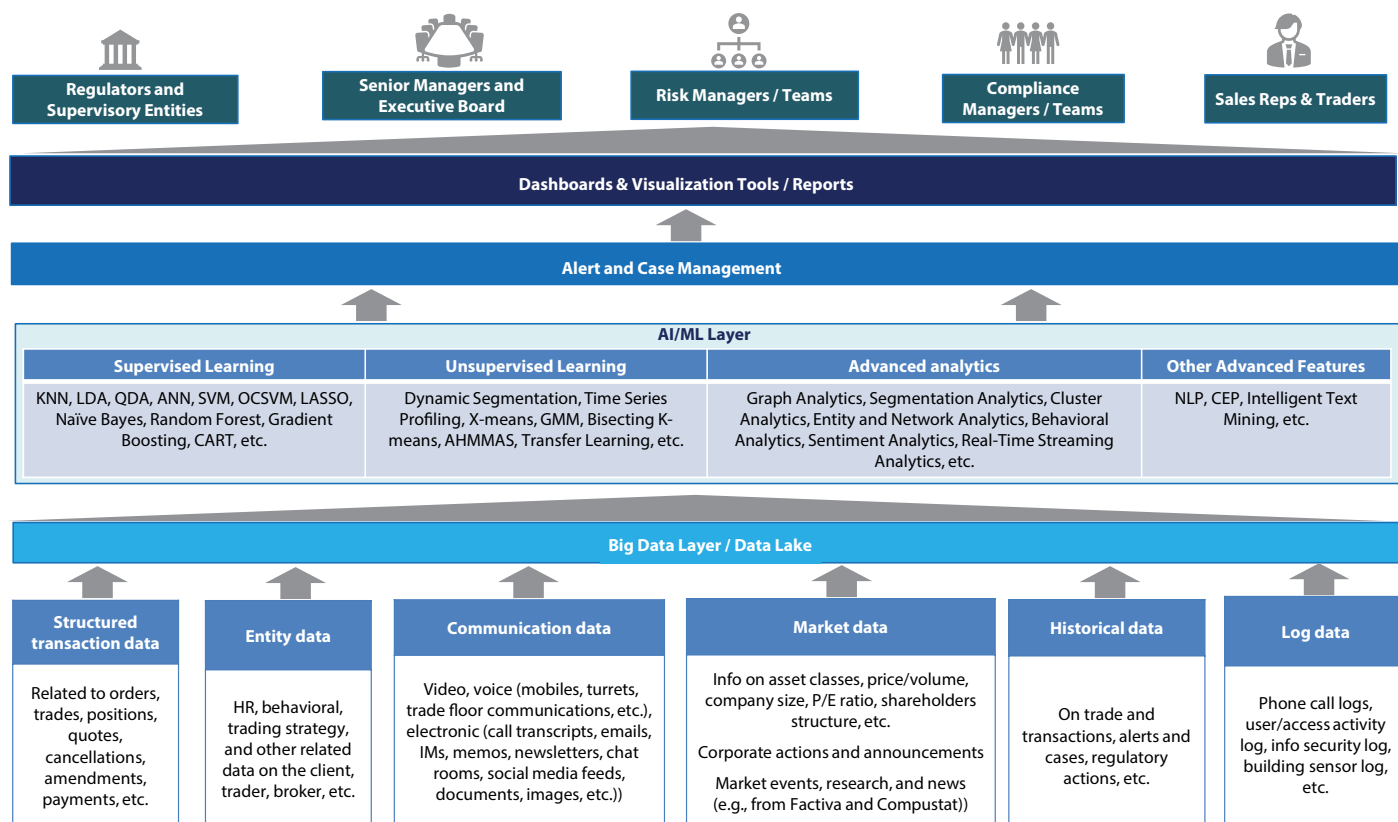


Figure 5: Illustrative Reference Architecture of AI/ML-Based Holistic Surveillance Solution

AI & ML in ORM — Real World Examples

Entity	Use Case	Elaboration
SIT & TradeFlow ¹	Operational Risk (OR) Measurement & Monitoring	TradeFlow and Singapore Institute of Technology (SIT) have collaborated to co-create an AI-driven solution to better address the operational risk and efficiency issues. They are leveraging AI and ML capabilities to monitor, measure, analyze, predict, and help manage the operational risk that a firm would face demurrage on shipments of bulk commodities across the world.
Yields.io ²	Model Risk Management	It has developed a model risk management (MRM) platform, called Chiron, that covers the entire lifecycle of model validation. The platform utilizes AI to enable ongoing model testing and validation on enterprise-wide scale. Further, it can integrate with graph databases, which enables users to better organize the MRM results. As per Yields.io, the platform helps reduce the cost of model validation by factor of 10.
Diligent ³	Third-party Risk Management (TPRM)	Its advanced ML and RPA-based solution can a) automatically detect unknown and known vendors by mapping against enterprise data sources; b) proactively identify potential for vendor failure; c) help automate entire TPRM life cycle (including onboarding, assessment, remediation, performance monitoring, and ongoing review); and d) accommodate evolving TPRM risk and regulatory landscapes.
FICO ^{4,5,6}	Cybersecurity Risk Management (CRQ and Residual Risk Mitigation Platform)	FICO released its ML-based Cyber-Risk-Score on AWS Marketplace. The solution's scoring-algorithm leverages new globally collected micro-signal data that improves the ability to quantify the cyber-risk of an enterprise in the next 12-months. The solution also offers supplementary-security-risk indicators which are especially valuable in evaluating small and medium-sized businesses. The solution offers sophisticated workflows and dashboards to stratify, compare, and manage aggregate- cybersecurity-risk.
Zero Networks ⁷	Cybersecurity Risk Management (zero trust security)	Its solution, called "Zero Networks Access Orchestrator", utilizes AI to enable zero-trust network-model. The platform observes how the users and machines typically communicate, and automatically defines and enforces a zero-trust network-model across enterprise.
Feedzai ⁸	Financial Crime Risk Management (fraud prevention)	Its ML-based platform can compute risk score in three milliseconds, evaluating 1000s of decisions to score a transaction in real-time. The solution's ML-models can identify patterns in transactions by analyzing customer profiles and behaviors; and leveraging external and third-party data.
AUSTRAC ⁹	Financial Crime Risk Management (KYC and AML)	In Australia, AUSTRAC (Australia's financial-intelligence agency), with the help of RMIT University researchers, have enabled AI/ML tools for the detection of suspicious activity. The solution can speedily and accurately unearth unknown money- laundering networks, and precisely and efficiently flag the transactions that require further investigation.
SAS ¹⁰	Financial Crime Risk Management (KYC and AML)	SAS AML solutions helps FIs to reduce false-positives up to 80%, achieve over 90% model-accuracy, and improve the SAR conversion-rate fourfold. The solution leverages AI and ML capabilities, and speedily processes massive amount of data. SAS has leveraged advanced analytics and ML capabilities to offer more configurable and intuitive investigation architecture; and support real-time screening capabilities. The solution can detect beneficial-owners, sanctioned-entities, and linkages in real time. SAS has also utilized RPA for AML investigations — which has helped minimize manual errors and decrease case review time by 20–30%.

Nasdaq ^{11,12,13}	Financial Crime Risk Management (holistic market surveillance)	Nasdaq SMARTS leverage AI and ML capabilities — over structured data (like orders, amendments and cancellations) and unstructured data (like electronic communications) — to achieve 360-degree holistic market surveillance. Further, Nasdaq has been investing substantially on enhancing the SMARTS solution — such as enabling new ML-based detection models; strengthening behavioral profiling and clustering, data discovery, and contextual surveillance capabilities; and leveraging ML for alerts ranking and scoring.
NICE Actimize ¹⁴	Financial Crime Risk Management (communications surveillance)	NICE Actimize SURVEIL-X Communication solution leverages ML, NLP, and other advanced capabilities to offer comprehensive communication surveillance of all regulated employee in a single cloud-ready solution. The solution surveils across communication modes (IM, chat, email, documents, social media, voice, desktop phones, turrets, mobile, video, etc.) and in several asset classes and languages.
NICE Actimize ^{15,16}	Financial Crime Risk Management (Regulation Best Interest (BI) compliance)	NICE Actimize's Reg BI Surveillance solution — which is part of its SURVEIL-X Holistic Surveillance platform — leverages NLP and ML capabilities and vast array of out-of-the-box-models to surveil 100% of all broker-dealer conversations and transactions. It automatically analyzes the disclosures and recommendations communications (both voice and electronic) of broker-dealers and raises alert.
FCA ¹⁷	Financial Crime Risk Management (surveil financial advisors conduct)	In UK, FCA has experimented with the usage of supervised learning and random forest techniques for predicting the probability of financial products mis-selling by financial advisors
Credit Suisse ¹⁸	Financial Crime Risk Management (trader surveillance)	Has partnered with Palantir to track rogue traders — the solution utilizes big data and AI/ML technologies. Note: Palantir also had a multi-year deal with U.S. SEC to help identify cases of insider trading.

Conclusion

In coming times, the usage of AI and ML by FIs for ORM is expected to increase significantly. Moreover, these new-age technologies would become a central element of an FI's future ORM strategy.



Acronyms

Acronym	Expansion	Acronym	Expansion
AI	Artificial intelligence	IVA	Intelligent Virtual Agent
AHMMAS	Adaptive Hidden Markov Model with Anomaly States	KNN	k-Nearest Neighbors Algorithm
AML	Anti-Money Laundering	KYC	Know Your Customer
ANN	Artificial Neural Network	LASSO	Least Absolute Shrinkage and Selection Operator
APT	Advanced, Persistent Threat	LDA	Linear Discriminant Analysis
AT	Algorithmic Trading	LOB	Line of Business
ATO	Account Takeover	ML	Machine Learning
CAIDA	Center for Applied Internet Data Analysis	MRM	Model Risk Management
CART	Classification and Regression Trees	NIST	National Institute of Standards and Technology
CAT	Consolidated Audit Trail	NLG	Natural Language Generation
CCAR	Comprehensive Capital Analysis and Review	NLP	Natural Language Processing
CDD	Customer Due Diligence	NLU	Natural Language Understanding
CEP	Complex Event Processing	OCSVM	One Class Support Vector Machine
CFO	Chief Financial Office	OFAC	Office of Foreign Assets Control
CIO	Chief Information Officer	OR	Operational Risk
CISO	Chief Information Security Officer	ORM	Operational Risk Management
CRQ	Cyber Risk Quantification	PCI DSS	Payment Card Industry Data Security Standard
CTR	Currency Transaction Report	PEP	Politically Exposed Person
DARPA	Defense Advanced Research Projects Agency	PGM	Probabilistic Graphical Models
DFAST	Dodd-Frank Act Stress Testing	PMML	Predictive Model Markup Language
DGA	Domain Generated Algorithm	QDA	Quadratic Discriminant Analysis
EDD	Enhanced Due Diligence	Reg BI	Regulation Best Interest
ERP	Enterprise Resource Planning	RPA	Robotic Process Automation
EU	European Union	SAR	Suspicious Activity Reporting
FCRM	Financial Crime Risk Management	SEC	U.S. Securities and Exchange Commission
FI	Financial Institution	SLA	Service-Level Agreement
GA	Genetic Algorithm	STOR	Suspicious Transaction and Order Report
GMM	Gaussian Mixture Model	STR	Suspicious Transaction Reporting
HFT	High-Frequency Trading	SVM	Support Vector Machines
HMM	Hidden Markov Model	TES	Triple Exponential Smoothing
IAM	Identity and Access Management	TM	Transaction Monitoring
IoT	Internet of Things	TPRM	Third Party Risk Management
ISO	International Organization for Standardization	UBO	Ultimate Beneficiary Owner

About the Author



Anjani Kumar

Principal Consultant in the Global Risk & Regulatory Technology Practices of Infosys Financial Services Domain Consulting Group.

Anjani has over 20 years of comprehensive experience in IT, domain, and process consultancy. He manages several strategic initiatives including thought leadership showcasing, solution enablement support, research and competency development program, and marketing efforts from a domain perspective. He has authored large number of whitepapers and articles; including many that have been published on reputed external forums.

References

1. [SIT and TradeFlow collaborate to enhance shipping industry efficiency with AI](#), Dec 6, 2021, [finance.yahoo.com](#).
2. [Model validation service of the year – Yields.io](#), Jun 24, 2020, [risk.net](#).
3. [Diligent Named a Leader in 2021 Gartner® Magic Quadrant™ for IT Vendor Risk Management Tools for Fourth Consecutive Year](#), Sep 2, 2021, [financialpost.com](#).
4. [Fico says latest fraud model helps identify 50% more scam transactions](#), May 26, 2021, [finextra.com](#).
5. [Advance AML Compliance with Artificial Intelligence](#), T J Horan, Frank Holzenthal, Dr. Scott Zoldi, 2017, [markomate.com](#).
6. [AI Meets AML: How the Analytics Work](#), Scott Zoldi, Feb 15, 2017, [fico.com](#).
7. [Zero Networks](#), [zeronetworks.com](#).
8. [Feedzai Fraud Detection Platform Uses AI, Biometrics](#), Sep 19, 2021, [nanalyze.com](#).
9. [New software to detect money laundering](#), Aug 20, 2018, [arc.gov.au](#).
10. [AML solution of the year: SAS](#), Keith Swanson, Sep 25, 2020, [risk.net](#).
11. [Changing The Game: Artificial Intelligence In Market Surveillance](#), Tony Sio, Apr 5, 2017, [nasdaq.com](#).
12. [The future of trade surveillance – Separating the Spoof from the Truth](#), [therealizationgroup.com](#).
13. [NASDAQ AND DIGITAL REASONING ESTABLISH EXCLUSIVE ALLIANCE TO DELIVER HOLISTIC NEXT GENERATION SURVEILLANCE AND MONITORING TECHNOLOGY](#), Feb 23, 2016, [ir.nasdaq.com](#).
14. [Comprehensive Communications Surveillance and Risk Detection](#), [niceactimize.com](#).
15. [Surveil-X Regulation Best Interest Surveillance](#), [niceactimize.com](#).
16. [NICE Actimize Introduces Innovative Reg BI Surveillance Solution to Help Organizations Comply with SEC's New Regulation Best Interest](#), Aug 12, 2019, [niceactimize.com](#).
17. [FSI Insights on policy implementation No 9: Innovative technology in financial supervision \(suptech\) – the experience of early users](#), Dirk Broeders, Jermy Prenio, July 2018, [bis.org](#).
18. [Credit Suisse teams with Palantir to sniff out rogue staffers](#), Mar 23, 2016, [finextra.com](#).

For more information, contact askus@infosys.com



© 2022 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.