Published August 2025

Compliance AI 9-Box Blue-Print

This article is authored by an Executive Advisor of Alberta Advisory and is sponsored by Madfoatcom.

The Material Stakes

Various industry reports (e.g. Thomson Reuters, Finantrix, Oliver Wayman) estimate the annual cost of compliance to be 10-15% of a bank's annual operating expenses. A material portion of annual compliance cost is dedicated to financial crime fighting (FCF) including- sanction screening, anti-money laundry (AML), counter fraud and combating terrorist financing (CTF).

Should we postulate that FCF consumers 5% of total operating expenses of a mature bank, then apply that to the Top-3 banks in each of the Gulf Cooperation Council (GCC) leading economies of KSA, UAE and Qatar, we arrive at an annual FCF spend of a whopping USD 1.1 B.

A precursory examination of the same countries' regulatory enforcement registers reveals the total penalties imposed on leading banks during the period 2022-2024 (inclusive) to be circa USD 15 M. Majority of these penalties pertain to FCF.

Intuitively, banks must continuously enhance their FCF frameworks to drive efficiency (e.g. reduce cost of compliance as a percentage of revenues) and effectiveness (e.g. eradicate violations).

In this article, we explore how Artificial Intelligence (AI) can help achieve that.

All rights reserved Alberta Advisory ©

The 9-Box Blueprint

Component	Proven Themes	Industry Citation
KYC / Profiling	a. Enrich counterparty profiles with analysis of social media content to infuse behavioral (e.g. PEP or POI affiliations) and motivational (e.g. philanthropy, greed) indicators. b. Enrich counterparty profiles with analysis of external content (e.g. court rulings, arbitration decisions, investigations) which is likely to impact credit score or ratings. c. Enrich counterparty profiles with dynamic investment and spending thresholds driven by past behavior (e.g. high value overseas remittances for tuition payment).	JP Morgan Chase uses its AI-Driven Contract Intelligence (COIN) platform to analyze legal documents, extract entity data, and update KYC profiles in real-time. For example, COIN unveils 150 pieces of information in commercial loan documentation (e.g. maturity, covenants). JP Morgan Chase developed COIN based on its proprietary AI platform called OmniAI using a mix of Natural Language Processing and Unsupervised Learning methods.
Graphing	d. Examine large volumes of data to identify direct and indirect connections between various counterparties (e.g. customers, guarantors, representatives, custodians) which can be exploited for financial crime (e.g. layering technique of money laundry).	Standard Chartered bank uses AI-driven network analysis to identify high-risk clusters of customers carrying out suspicious transactions. Standard Chartered uses SAS Technology to achieve that.

All rights reserved Alberta Advisory ©

Component	Proven Themes	Industry Citation
	e. Prioritize the connections based on transaction frequency, value and risk ratings.	
Risk Ratings	f. Dynamically adjust the Risk Rating of customers using richer financial data (e.g. cash flow anomalies, net worth indicators) and non-financial data (e.g. business activities declaration, published career and education data).	Deutsche Bank uses AI to screen provided Identification documents (e.g. driving license, utility bills) to protect against identity theft
Transaction Screening	g. Risk rate a transaction in real time using a risk probability model, rather than, a rule-based engine. The probability model is tailored to specific segments, customers, products and time.	Citi Smart Match system fetches transaction histories and geo locations to rank payment transactions (risk-wise) on a scale from 0-999 and blocks transactions after matching certain thresholds that are customer-specific. The system was trained on billions of transactions to detect exceptions n less than 50 milliseconds. Examples include- larger than usual transfers, new suspicious beneficiaries, disparately located closely timed payments, etc.
False Positive Optimization	h. Provide a feedback loop to Transaction Screening system to filter out false positives based on cases investigated manually and proven to be safe. For example, ignore high spend airline ticket card	HSBC partnered with Qauntexa to deploy their contextual intelligent decision-making platform. This is used to distinguish between legitimate complex behavior and genuinely suspicious

All rights reserved Alberta Advisory ©

Component	Proven Themes	Industry Citation
	transactions for a customer who frequently travels during the Summer.	activity, dramatically reducing false alerts in their AML monitoring
Document Inspection	i. Use a product-trained Natural Language Processing (NLP) model to vet and validate documents by looking for specific tokens (i.e. key words) relevant to that banking product. For example, matching the information of a Letter Of Credit (LC) to supplied bills of landing, shipping manifests, invoices and insurance policies.	OCBC (Singapore) AI system can process complex trade documents in minutes instead of days, checking for over 90% of discrepancies automatically. The system was developed by AIDA Technologies (later acquired by Ant Group) and combines Computer Vision, Deep Learning, Optical Character Recognition and NLP technologies.
Threat Intelligence	j. Use unsupervised learning models to learn how bank's physical assets and users behave then, detect any exceptions that may signal stealth attacks. The behavior modeling includes- usage seasonality, usage frequency, usage cross-relationships, geo locations, IP addresses, etc. This specifically applies in case of "Advanced Persistent Threats – APT" and newly threat scenarios reported by international bodies such as- FS-ISAC, MISP and AlienVault OTX).	HSBC partnered with Darktrace to uncover subtle network intrusion attacks. Darktrace's "Enterprise Immune System" learns the unique "pattern of life" for every user and device on HSBC's vast network and report accumulated deviations over time that may signal an APT.
Operational Risk Assessment	k. Use predictive modeling to estimate the operational risk exposures of a bank, a line of business or a product by analyzing historical data of- key risk	Standard Chartered Bank uses SAS Operational Risk Management platform to automate the core risk governance and control processes across its international

All rights reserved Alberta Advisory ©

Component	Proven Themes	Industry Citation
	indicators (KRIs), risk control self-assessment (RCSA) and reported losses.	network, then applies predictive analytics to forecast loss event frequency and severity.
Suspicious Activity Reports (SAR)	l. Use of Generative AI and AI-empower search to collect all relevant information pertaining to a specific compliance case then, generating regulatory disclosures.	Morgan Stanley uses OpenAI platform to search large corpus of bank's data (e.g. policies manuals, transactions, emails) and generate draft compliance memos and reports for later review by compliance department.

Thanks!

All rights reserved Alberta Advisory ©

Disclaimer:

This article provides the personal views of the author. The words and other content provided in this article, and in any linked materials, are not intended and should not be construed as investment, financial, consulting or otherwise advice.

While the author has exercised diligence in the collection, analysis and representation of the business and market information provided, the author and the sponsor disclaim any and all liability in the event any information, commentary, analysis, opinions, advice and/or recommendations contained in this article prove to be inaccurate, incomplete or unreliable, or result in any tangible intangible or otherwise damages.

All rights reserved Alberta Advisory ©