INTESA SANPAOLO

L'evoluzione dei sistemi di monitoraggio transazionale in Intesa Sanpaolo

Luca Cattarossi – Senior Director
Resp. Servizio Monitoraggio Transazionale AML
Direzione Anti Financial Crime
Intesa Sanpaolo

Roma, 4 novembre 2025

Il modello di presidio del monitoraggio transazionale

- **Il Modello di ISP Sanpaolo** per il Monitoraggio Transazionale AML è **formalizzato in apposite «Regole di monitoraggio transazionale e SOS»** e **si articola in macro processi**

Ambito	Macro processi
Sviluppo modelli TXM AML	• Risk assessment, coverage analysis e analisi di impatto • Data feeding, data mapping e data quality • Sviluppo e calibrazione degli scenari automatici; backtesting e lookback • Analisi e investigazioni speciali; governance e supervisione scenari
Alert e Case Management	• Analisi degli «alert» generati dai sistemi automatici, chiusura dei False positive ed escalation dei True positive (CC TXM AML 1L BSC) • Analisi dei «case» ed esecuzione di investigazioni speciali (CC TXM AML 2L AFC)
Segnalazioni di Operazioni Sospette	• Analisi segnalazioni di operazioni sospette di 1 livello di iniziativa rete o originate dal CC TXM AML • Valutazione posizioni da archiviare e da inviare alla UIF (SOS di 2 livello)
Processi, reporting e quality assurance	• Quality Assurance TXM AML • Adeguamento del sistema incentivante • Reporting direzionale ed operativo

L'evoluzione dei modelli applicati al Monitoraggio transazionale

Fasi di sviluppo

2019 - 2021

Parametrizzazione scenari e soglie applicazione Vendor Based (logica mono fattoriale)

- Costituzione «Quant OffIce» (2019)
- Monitoraggio singoli rischi su scenari «rule based»
- Estensione al Gruppo dell'applicazione Vendor Based
- Personalizzazione estesa e centralizzata (logiche, calibrazione parametri, segmenti di clientela)

2022 - 2024

Aumento coverage analysis con logiche multifattoriali

- Progettazione ed estensione scenari proprietari con logiche multifattoriali
- Progettazione logiche di intercettamento evolute (Consorzio AFC Digital Hub)
- Adozione di investigazioni speciali, anche ad esito della partecipazione ai Partenariati Pubblico Privati (EFIPPP – Europol)
- Prima validazione Modello TXM AML (marzo 2024)

2025 - 2026

AFC Model risk management e applicazione AI

- Adozione primo scenario con logiche di artificial intelligence (MAD contante)
- Estensione attesa sul 2026 dei modelli AI (es. bonifici e Isybank)
- Adozione di un framework di AFC Model Risk Management
- Scoring comportamentale e lavorazione differenziata alert

Sviluppo scenari AI based – MAD contante

Logiche di progettazione e risultati in produzione

Logiche di progettazione e di roll-out

- Selezione di circa **100 features su elementi di natura oggettiva** a copertura dei red flag UIF (anomalie volumetriche, velocity, anomalie temporali e sequenziali)
- **Sperimentazione di 4 algoritmi** di anomaly detection di tipo unsupervised machine learning, con **scelta di Local Outlier Factor**
- Elaborazione di un **ranking di anomalia comportamentale** di ogni account considerato
- **6 mesi di pilota** (su un campione limitato di alert) prima della messa in produzione realizzata a Settembre 2025

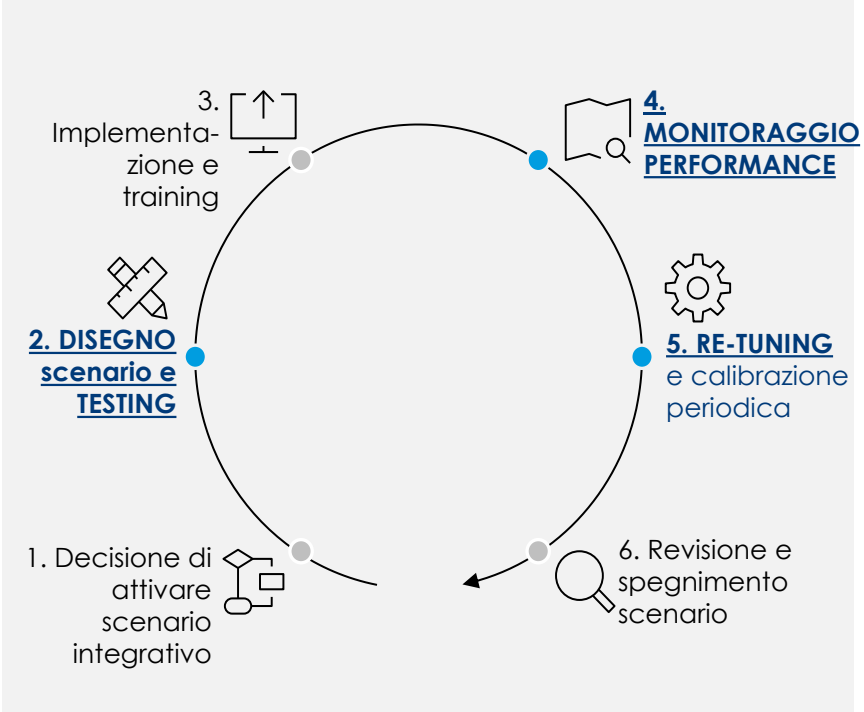
Risultati in produzione

- **Limitata regressione sulle SOS** originate dai sistemi rule based
- **Notevole progressione** (**50x**) delle **SOS prima intercettate dalla rete territoriale** e non intercettate dagli algoritmi rule based
- Tasso di **true positive 10x sul periodo pilota**
- Mantenimento di un **modello ibrido**, con disattivazione di gran parte degli scenari rule bases sul contante e mantenimento selettivo di alcuni scenari (es. scenari che monitorano le operazioni di prelievo e di versamento di elevato importo)

Adozione di un framework di AFC Model Risk Management (1/2)

Ciclo di vita di un modello di TXM AML e utilizzo delle metriche

Ciclo di vita di uno scenario TXM AML



Uso di metriche (target e limiti) nelle varie fasi

DISEGNO scenario e TESTING

- Durante la fase di test e convalida di nuovi scenari è necessario calcolare (su base campionaria) i principali indicatori di performance
- Il confronto con gli obiettivi e i limiti consente di approvare le modifiche al modello

MONITORAGGIO PERFORMANCE

- Le metriche vengono calcolate e confrontate con gli obiettivi e i limiti su base continuativa

RE-TUNING E CALIBRAZIONE PERIODICA

- Il monitoraggio regolare fornisce input al processo di messa a punto e ricalibrazione, identificando le aree in cui è necessaria una messa a punto a causa di prestazioni insufficienti.
- Un processo di monitoraggio robusto consente potenzialmente di passare da una messa a punto annuale a una messa a punto basata sugli eventi

Adozione di un framework di AFC Model Risk Management (2/2)

Metriche per categoria e finalità

Categoria	Finalità	Metriche (estratto)
1.Volume	• Monitoraggio evoluzione dati andamentali macro	• N e volume transazioni per Business Unit • Incidenza alert / transazioni • Incidenza alert / base clienti
2. Performance operativa	• Controllo arretrati (stock e backlog) • Controllo tempistiche di lavorazione	• Valore stock e backlog e rapporto relativo • % alert chiusi dopo 60/90 gg • % SOS inviate dopo 90 gg
3. Risk Coverage	• Misurazione del grado di copertura dei rischi AML (red flag)	• % di coverage da controlli manuali • % di coverage da controlli automatici
4. Efficienza	• Misurazione del grado di efficienza del modello TXM AML • Misurazione del grado di efficienza dei singoli scenari	• % Veri positivi intercettati dal CC TXM AML (1° e 2° livello) • % complessiva alert che diventano SOS (SAR escalation rate) – totale e per scenario
5. Efficacia	• Misurazione dell'efficacia del modello (minimizzando le SOS non intercettate dai sistemi in essere) • Misurazione dell'efficacia dei singoli scenari	• Analisi campionarie «sotto la linea» (BTL) • Analisi causa radice delle SOS ad alto rischio di provenienza rete non intercettate dai sistemi automatici

Temi prospettici di evoluzione del modello (1/2)

- Mantenimento di un **modello ibrido** (scenari Rule based e scenari AI based) superando il concetto di «NO SAR left behind»); **shift su un modello puro «AI Based»** da valutare in base alle evoluzioni della tecnologia e agli esiti delle analisi di non regressione
- Integrazione **dati dal dominio Anti Fraud e Cyber**
- Sperimentazione **tecniche di LLM e RAG nella filiera end-to-end** (anomaly detecion, decisione informativa, documentazione dei risultati) con **«Human in the loop»**
- Potenziamento delle logiche di **scoring comportamentale** per indirizzare **modalità differenziate di lavorazione degli alert** (ibernazione, lavorazione ordinaria, lavorazione rafforzata con tecniche di network analysis)

Temi prospettici di evoluzione del modello (2/2)

Potenziamento delle logiche di **scoring comportamentale con adozione di soluzioni di AI** per indirizzare modalità differenziate di lavorazione degli alert **(approccio risk based), con recuperi di efficacia ed efficienza**