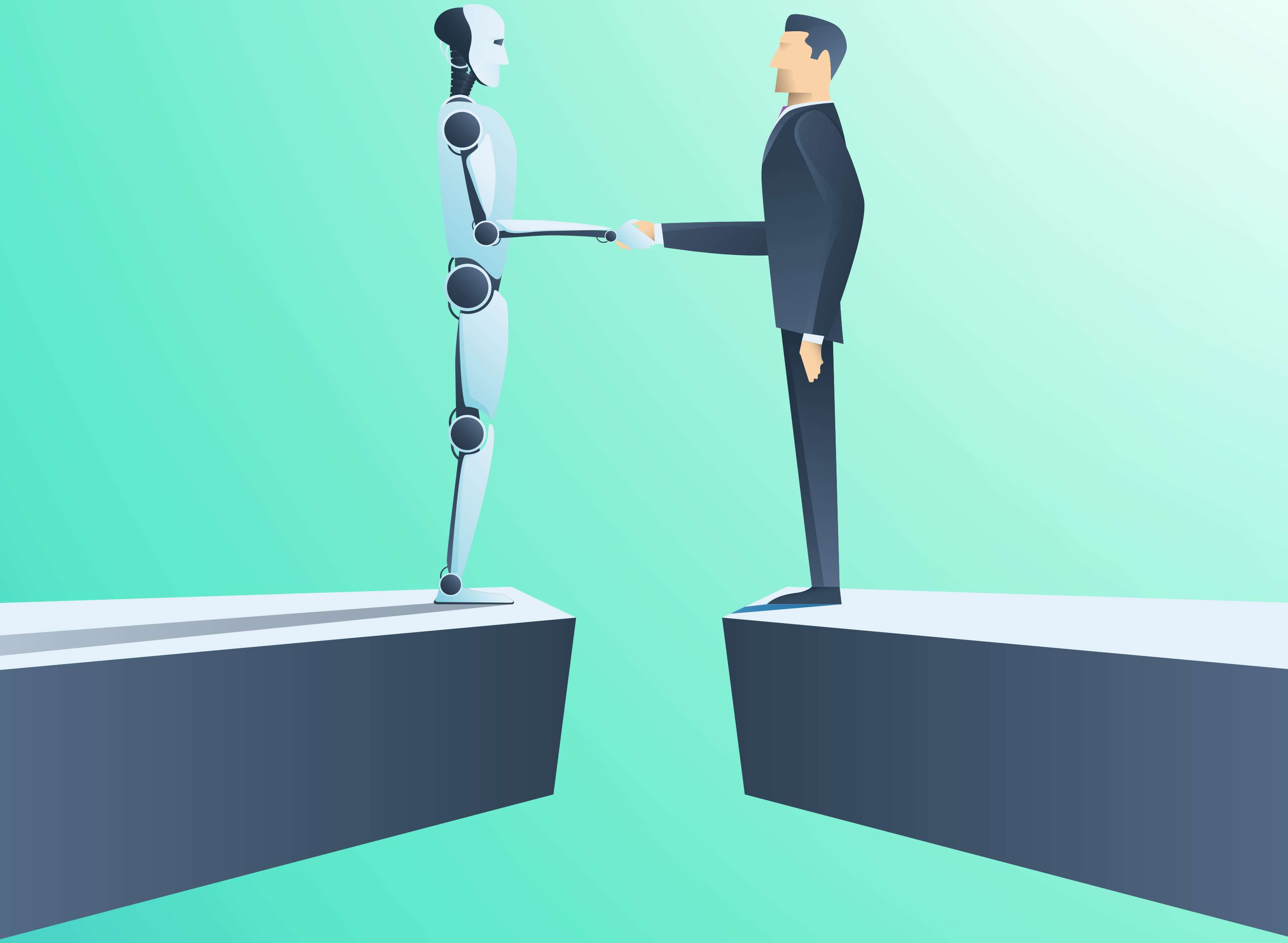
Connected World.
Connected Experiences.

Tech Mahindra
BUSINESS PROCESS SERVICES

COGNITIVE AUTOMATION FOR OPERATIONAL RISK MANAGEMENT

AI BASED PROCESS SURVEILLANCE IN TRADE LIFECYCLE

BY - NEERAJ PARASHAR



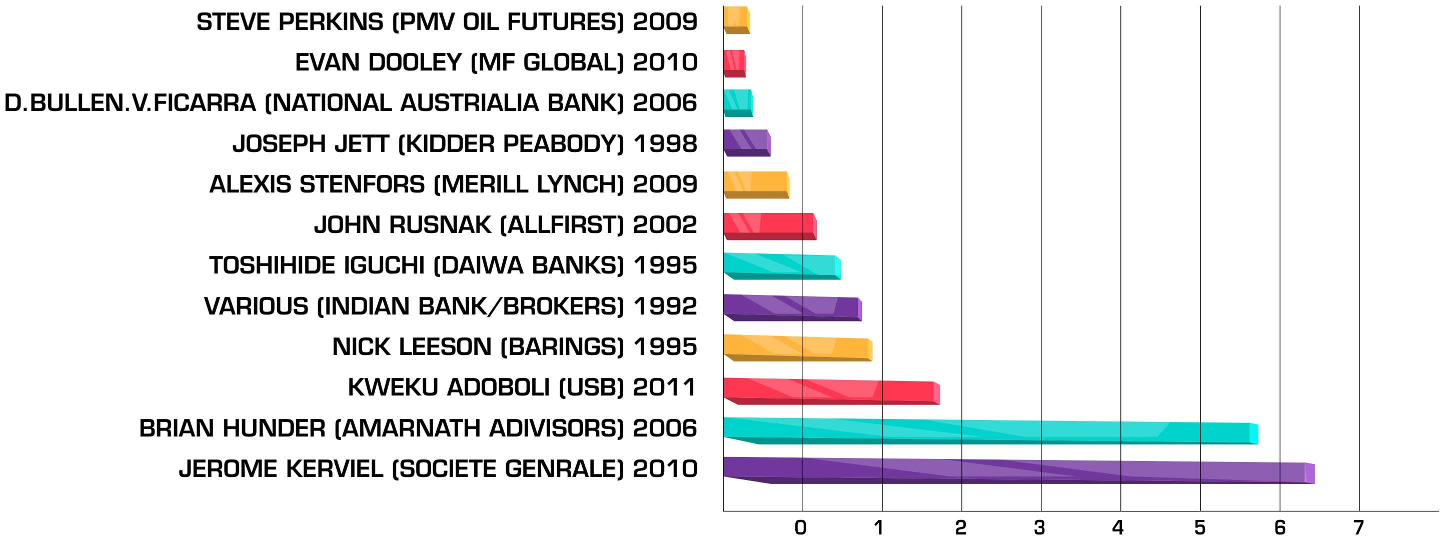
“Originally published in August 2018 Edition of the Shared Services Forum Journal, 'Process Edge' (copyrighted)”

AI BASED PROCESS SURVEILLANCE IN TRADE LIFECYCLE

In recent times, leading global banks have drawn attention towards trading patterns where an individual employee has the ability of putting the financial position of the banks or trading houses at risk. This is commonly referred to as Rogue Trading. Rogue trading has largely been possible due to limited awareness towards risk-based scenarios and vulnerable organization practices, paving an easy way towards such outcomes. With likelihood of cybercrime and ransomware, there is a huge risk involved where any single act of such practice can convert the capitalization of any bank or financial institution to a significantly low level and impose existential threats in terms of direct financial exposure, loss of customer base or huge penalties.

The risk of rogue trading can be effectively mitigated early on by warning signals flagged off by AI based cognitive RPA that helps to prevent occurrence of such scenarios from the system. The table below specifies the top financial losses which were caused directly by rogue trading between the period 1992 and 2011.

ROUGH TRADING INDUCED APPROXIMATE LOSS IN $ BILLIONS



The case of Nick Leeson requires special mention which led to Baring Bank's eventual insolvency. He brought down the 233 year old Barings Bank to a third of its capitalization. Its losses on unauthorized investments in index futures contracts were sufficient to bankrupt the bank in 1995. Through a combination of poor judgement on his part, increasingly large initial profits, lack of oversight by the management, a naive regulatory environment, and an unforeseen outside event - the Kobe earthquake, Leeson incurred a US$1.3 billion loss that bankrupted the centuries old financial institution.

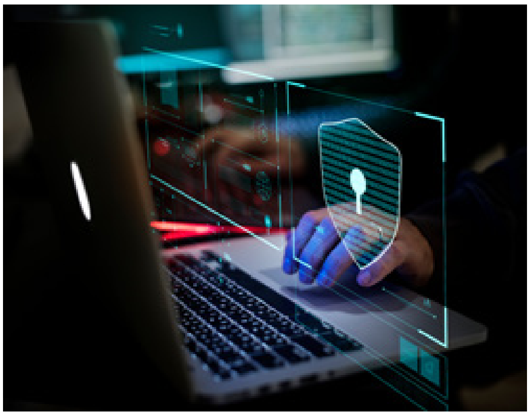
RISK OF ROGUE TRADING

In the world of data protection accountability with mandatory compliance of GDPR like regulations, organizations are more vulnerable to unauthorized access from inside, than external data breaches.

Rogue trading is one such scenario which is high stake and prone to high risk, high tension and high frequency. The operational dangers inherent in the world of securities and derivatives trading have risen dramatically in last 20 years with operations becoming digital.

This new threat is a result of the advent of high-frequency, black box' trading strategies, which are fully automated but not fully optimized, for the low latency exchange markets. In the past, traders would exceed limits, and finding prices moving against them, extend their unauthorized positions. The build-up of risk and losses would force the individuals to cover up and misrepresent activities. Such hidden positions, when brought to light, have toppled banks, and led to resignations of senior executives with otherwise stellar records. In the future, banks, or worse — clearing houses — could be brought down by high-frequency trading software building massive positions in unforeseen and difficult to predict ways.

The black box rogue trading scandal of the future will have much in common with the rogue trader scandals of the past. The actions of those individuals dubbed as 'rogue traders' have fascinated and, to an extent, invoked a degree of awe and admiration from those not directly affected by their machinations. These individuals circumvented controls, exceeded limits, and carried on by misrepresenting their holdings and risk. Unfortunately, in the high-stakes, high-risk, high- tension world in which traders find themselves, the drive for success can overcome ethics. These individuals cover losses and deceive their colleagues, often in clever and ingenious ways. After the blow-up, it usually turns out that rogue traders have exploited multiple weaknesses in their firms' procedures and systems. Keep in mind as well, that in most cases, investigations reveal that a number of managers were aware of the profits (which later, of course, turn out to be fictitious), and therefore the risks that were being taken.



KEY QUESTIONS FOR RISK MANAGEMENT

In the digital ecosystem, there are many automated activities, which require regular reviews and governance to reduce risk exposure. Some of the important questions to be asked are listed below:

- **Are banks running 'stress tests' on their high frequency trading programs?**

- **Could errors in price feeds from the many sources of market data trigger a flood of trades before the aberration is detected?**
- **Could detailed knowledge of a large bank's algo trading rules be exploited by an external trader who sets off the market conditions that lead the algo to 'misbehave' or 'go rogue'?**
- **Are regulatory cross-market 'circuit breakers' and trading halts required, or can natural price discovery be retained in today's low-latency markets?**

Concerns around the role of these algorithms skyrocketed after the so-called 'flash crash' of 6th May 2010 that caused the Dow Jones Industrial Average to plunge nearly 1,000 points in less than a half hour, with nearly a trillion dollars in stock market value evaporating — and then (mysteriously) reappearing. When it was later discovered that 68 percent of the questionable trades that ended up being cancelled involved Exchange-Traded Funds (ETFs) whose trading is highly computerized, the US regulators decided to explore whether algorithms that cause disruption in markets should be treated as if they were rogue traders.

Regulators are eager to develop methods for assigning responsibility when trading technology goes awry. Overall, the computerization of financial markets has improved transparency and efficiency, and reduced investors' costs. To avoid politically motivated bans on new trading technologies, leaders in the financial markets industry must define when high-frequency or algorithmic trading crosses the line into being disruptive to markets, and who is responsible when it happens. Finding the answers to these concerns is now perhaps the most critical element in ensuring the safety of financial systems in the future.

With a two-pronged approach of system audit and monitoring transactional data, AI-based cognitive RPA solutions via predictive model and proactive actions not only provide early warnings but also execute them automatically. The key benefits for the organization by installing such solutions are:

- **Stakeholder Value**
- **Corporate Governance**
- **Risk and Compliance**
- **Early Warning Signals**
- **Prevention of Financial loss**
- **System Robustness**

DIGITAL CAPABILITY FOR RISK MANAGEMENT

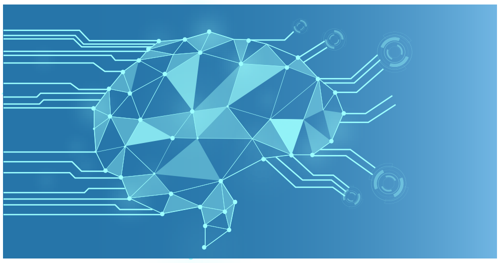
As per current circumstances, Blockchain, IoT and RPA are taking over human input based governance. There is very little room left in the process or system not monitored closely in an integrated architecture. To have such a robust capability, organizations need to have a clear view of not only their enterprise architecture i.e. SOA (Service Oriented Architecture) but also customer facing BPM platforms. There is a distinct possibility that agile enterprise changes may leave some risk controls open for future vulnerabilities. In light of such situations, AI-based capability is not only vital but imperative to have.

Business integration services are putting a 'method in the madness' by framing agreements for their partners and vendors. However, a huge area in operational environment is left unattended. In the digital world, old methods/ practices are not going to be replicated. With disruptive technologies and dynamic business environment, structured thinking based on concepts and lots of imagination is required to seek the necessary capability to meet internal and external threats and attacks.

CASE SCENARIO

Recently, a leading BPO company conducted a risk assessment exercise of many of its clients to identify vulnerable scenarios at client locations. Based on the learning captured, an AI-based solution was designed to mitigate all such scenarios in the future. While assessing the Trade to Settlement process on a client, the BPO Company observed that there are huge discrepancies in the system with respect to people, processes and technology. Based on preliminary suggestions, the client noted the hugely vulnerable circumstances of their processes the client decided to leverage the assessment to not only determine the loopholes but at the same time, take immediate preventive and corrective actions.

AI BASED DEEP LEARNING FRAMEWORK



Based on various scenarios, a pattern discovery analysis has been designed through multivariate and big data analytics that will identify the drivers (independent factors) of such instances and frame a predictive model for early warning signals and establish robustness of the system.

The key areas where the below methodology helped are:

- **Access Control Issues**
- **Technology Implementation in mapping business rules to accounting books**
- **Reconciliation Issues with respect to open exceptions**
- **No ownership and accountability against failed trades**
- **Discrepancy in Static and Reference Data**

AI-BASED SURVEILLANCE MECHANISM

Broadly the surveillance mechanism can be developed around two broad major dimensions:

1) Core Process Based Scenario Governance

2) Data Driven Discrepancies

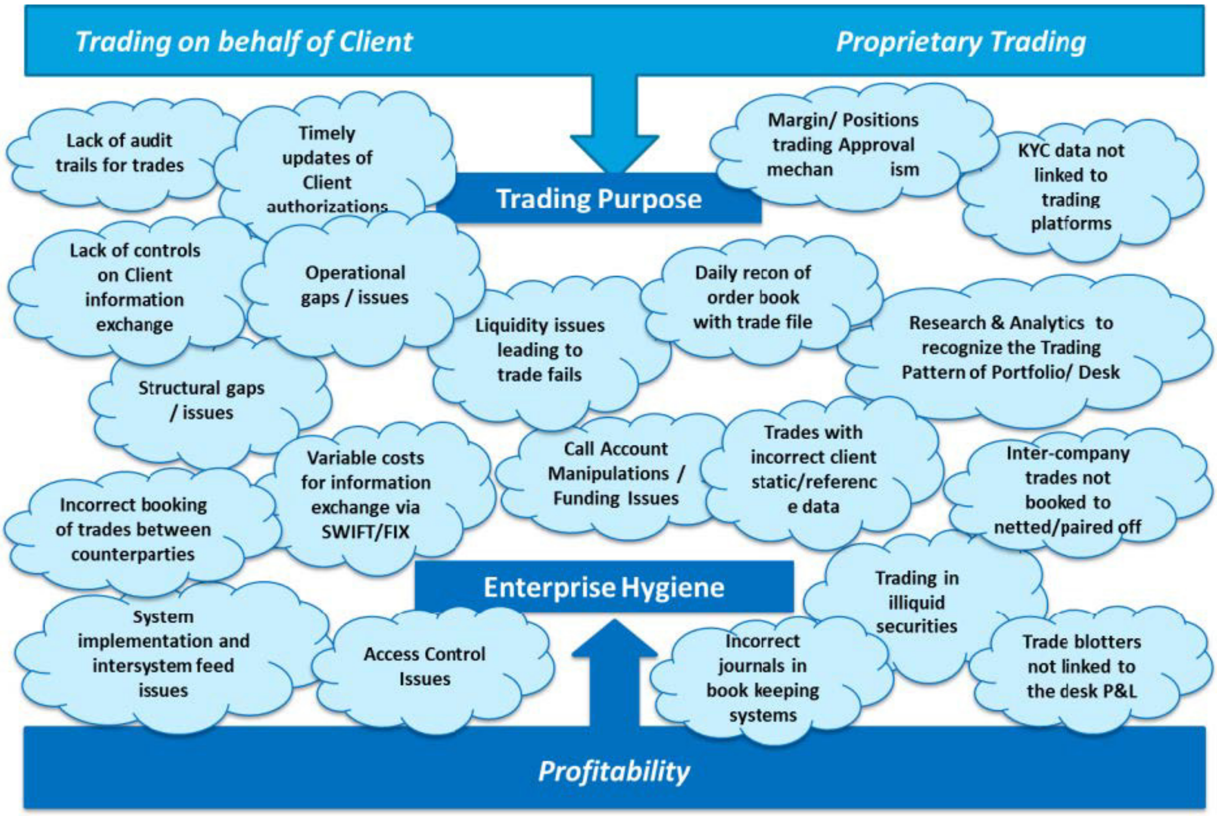
Core Process Based Scenario Governance (or System Audit Framework & Business Intelligence). Here, user stories and remedial actions need to be configured on the AI platforms as scenarios to put a robust and scalable governance mechanism in place.

The process and customer journey scenarios can be broadly classified into two categories:

1) Trading related scenarios where transaction level governance is required

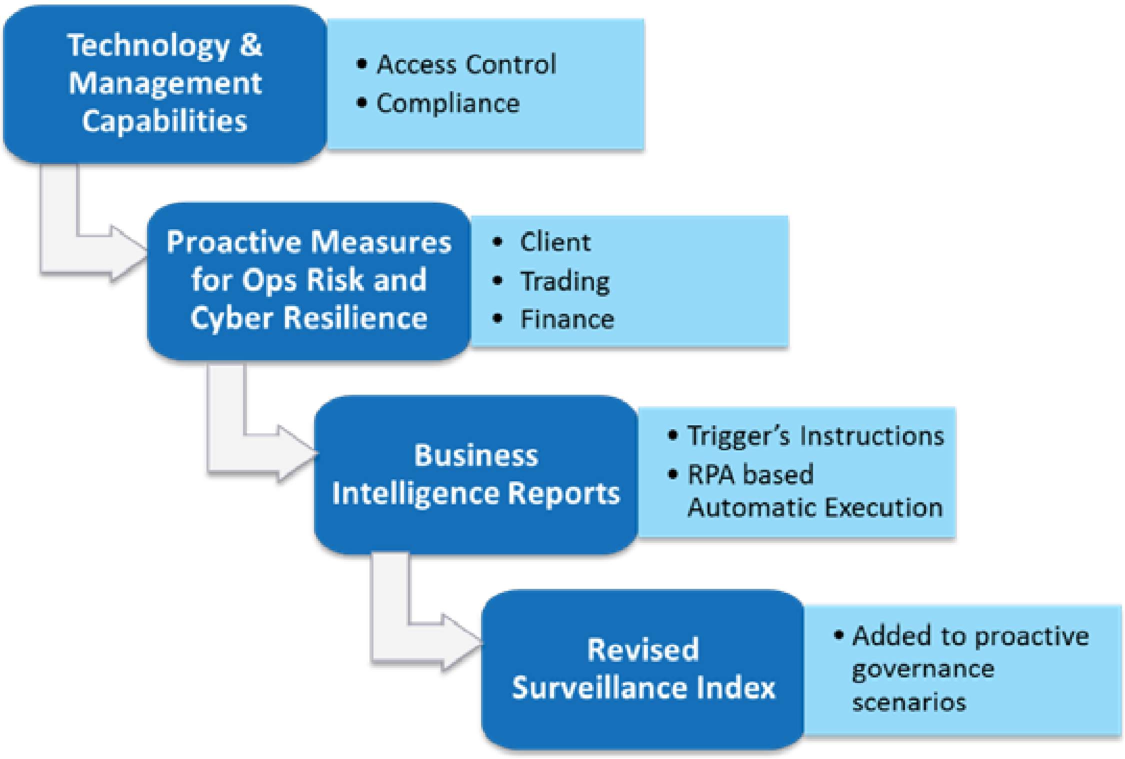
2) Enterprise security and hygiene, which requires significant specific security standards and framework based approach for sustained and consistent operational excellence

TRADE LIFE CYCLE RISK RECOGNITION ASPECTS: MAJOR SCENARIOS


Trading on behalf of Client
Proprietary Trading
Trading Purpose
Lack of audit trails for trades
Timely updates of Client authorizations
Margin/ Positions trading Approval mechan ism
KYC data not linked to trading platforms
Lack of controls on Client information exchange
Operational gaps / issues
Liquidity issues leading to trade fails
Daily recon of order book with trade file
Research & Analytics to recognize the Trading Pattern of Portfolio/ Desk
Structural gaps / issues
Variable costs for information exchange via SWIFT/FIX
Call Account Manipulations / Funding Issues
Trades with incorrect client static/referenc e data
Inter-company trades not booked to netted/paired off
Incorrect booking of trades between counterparties
Enterprise Hygiene
Trading in illiquid securities
System implementation and intersystem feed issues
Access Control Issues
Incorrect journals in book keeping systems
Trade blotters not linked to the desk P&L
Profitability

The two categories as above have their own specific elements but it is very essential to note that these two categories are interdependent, making the scenario complex, demanding digital capability to track and monitor risks from rogue trading.

In the next table, details of the major factors are mentioned, in terms of developing scenarios and incorporating controls in front, middle and back office.



Technology & Management Capabilities

- Access Control
- Compliance

Proactive Measures for Ops Risk and Cyber Resilience

- Client
- Trading
- Finance

Business Intelligence Reports

- Trigger's Instructions
- RPA based Automatic Execution

Revised Surveillance Index

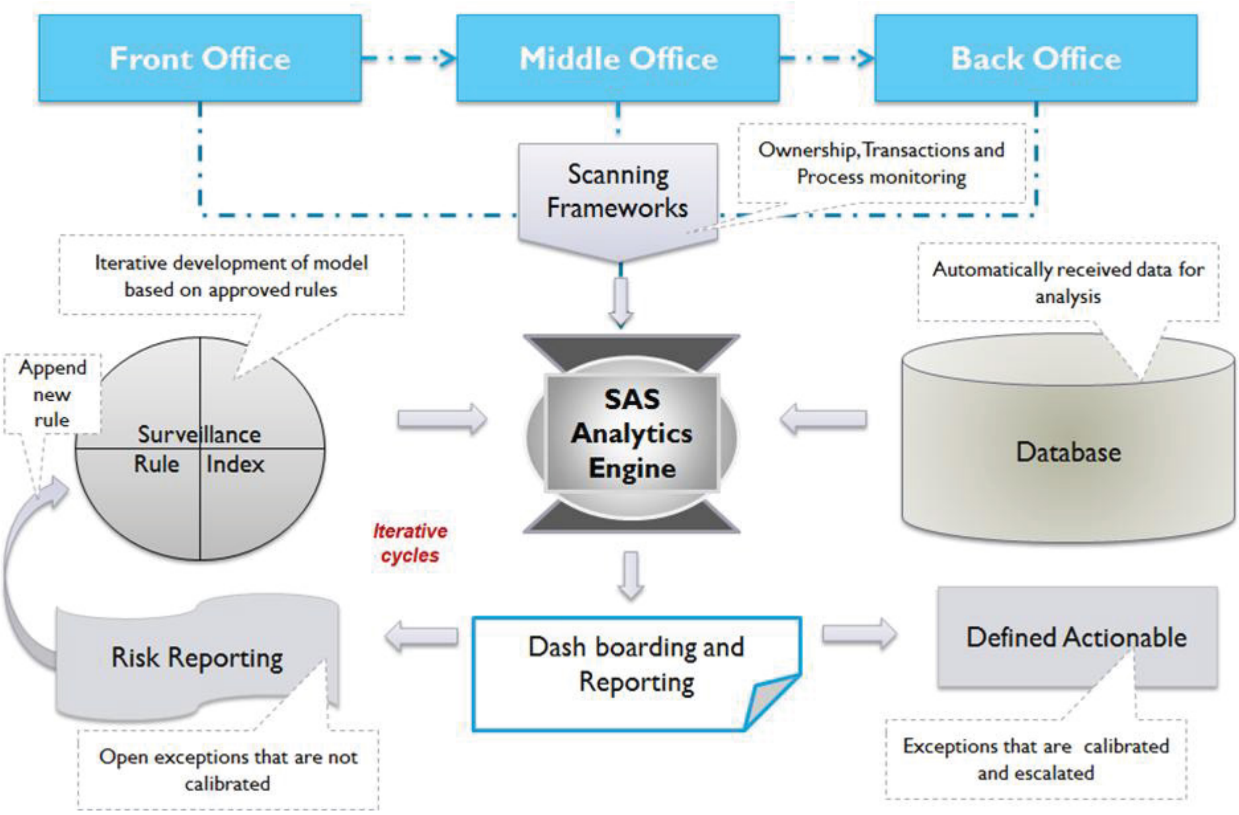
- Added to proactive governance scenarios

	Front Office	Middle Office	Back Office
TRADING SCANNER	▶ Purpose of Trading based on pattern recognition. ▶ Dealer Profile validation. ▶ Manual entry of counter party. ▶ One time vendor transactions, not in ICP master.	▶ Access of booking/capturing trades and settlement to same person. ▶ Confirmations are managed manually or can be influenced. ▶ Trade allocations to incorrect client/prop accounts. ▶ Confirmed trades are not pre-matched within stipulated timelines/matched incorrectly.	▶ Exceptions during settlement are incorrectly booked/settled. ▶ Failed trades are not reported on time/reported incorrectly. ▶ Failed trades are allocated to incorrect age/nominal buckets ▶ Accounting entries booked to incorrect journals
TECHNOLOGY SCANNER	▶ Existence of non-live portfolios. ▶ No-access control of S&R data. ▶ No call back to confirm static and reference data. ▶ No monitoring of trade patterns for inter-company trades	▶ Manual confirmation of trades. ▶ Manual pre-matching of trades. ▶ Manual release of trade instructions in the market . ▶ Manual reporting, tracking and monitoring of post trade events. ▶ Reconciliation rules not preset in systems.	▶ All Static Data is not aligned/ implemented to accounting events. ▶ All source applications are not aligned to FIs. ▶ All daily exceptions are not automatically flagged on time. ▶ All resolved exceptions are do not have audit trail. ▶ Reconciliation and fail reports are not automated.
FINANCE SCANNER	▶ No daily recon by system of all transactions booked by FO and closure of open issues. ▶ No ownerships of accountability issues ▶ No job swapping and risk audits pertain to operational practices and processes.	▶ All daily exceptions are not escalated or channelled to respective business owners. ▶ Root cause analysis not done on daily exceptions. ▶ All transactions are not tracked in book keeping system/ledgers	▶ Incorrect flow in the Inter-system reconciliation. ▶ Incorrect posting of journals leads to incorrect balances in the sub-account leading to contra bookings in the suspense and the wash accounts.
ACCESS CONTROL SCANNER	▶ Traders/Sales Desks having access to book keeping and settlement systems.	▶ Access control issue of call accounts & Bank Accounts. ▶ No clarity on creating, editing and deleting call accounts.	▶ Manual adjustment of accounts and database ▶ Back office personnel having access to trade booking / amendment systems.
CLIENT SCANNER	▶ No Audit trail of client requests. ▶ No tracking of client grievances. ▶ No system of clearing client accounts on periodic basis. ▶ No formal preset channel for client communication ▶ Client sensitive information sent to incorrect parties.	▶ Absence of formal communication for confirmation and settlement for all trades.	▶ No reverse recon for each client data via automatic mechanism.
COMPLIANCE SCANNER	▶ Movement of people from middle office and back office. ▶ No Tracking of financial impact in their dealings. ▶ No audit trail of employee access levels and internal account details.	▶ No planned rotation of people ▶ Existence of non-live employees in the system.	▶ Absence of external audit practices or strong internal audit.
EARLY WARNING SIGNALS SCANNER	▶ No Dash boarding system ▶ Recon between order book and trade book across applications	▶ No Dash boarding system ▶ Management of swift cost and offline trade separately.	▶ No Dash boarding system around critical parameters like Ratios , Performance and Pattern.
BUSINESS INTELLIGENCE SCANNER	▶ Movement of people from middle office and back office. ▶ No Tracking of financial impact in their dealings. ▶ Absence of trading pattern recognition software ▶ No strong follow up and closure	▶ Absence of analytics engine around defined business rules. ▶ No strong follow up and closure ▶ Separation of official duties. ▶ Conflict of interest.	▶ No analytics of data available in system ▶ No strong follow up and closure

DATA DRIVEN DISCREPANCIES or DATA DRIVEN ACTIONABLE INSIGHTS

These are descriptive, diagnostic, predictive and prescriptive analytics via actionable insights, KPI reports and models/patterns.

OFF-TRACK TRADING STRATEGIES – SURVEILLANCE MECHANISM


Front Office
Middle Office
Back Office
Scanning Frameworks
Ownership, Transactions and Process monitoring
Iterative development of model based on approved rules
Automatically received data for analysis
Append new rule
Surveillance Rule Index
SAS Analytics Engine
Database
Iterative cycles
Risk Reporting
Dash boarding and Reporting
Defined Actionable
Open exceptions that are not calibrated
Exceptions that are calibrated and escalated

CORE PREVENTIVE MEASURES

The major rogue trading cases discussed above were all avoidable through basic, general management governance and review. There are a few immutable principles in the control of trading operations, but management must enforce them rigorously and continuously with no exceptions. The four core principles for avoiding rogue trading disasters are as follows:

- **Separating front/middle/back office activities and processes. Segregation of duties ensures traders cannot interfere with the processing and reporting of their transactions**

- **Limiting access to trading, risk control and settlement systems to separate functional areas completely and preventing any individual from having access to more than one area**

- **Using independent, outside pricing sources for mark-to-market valuing of positions. It's easy to value a bank's position in IBM shares, but many traded instruments do not have an easily obtainable market price. Allowing internal staff to enter price estimates for profit and loss calculations opens the firm to deception**

- **Ensuring integrity, which is the key to a good trading system. This means all trade accounting data are accurate and consistent, and can be verified easily through reconciliation with external parties (e.g., client trade confirmations, clearing, etc.**

In summary, firms must maintain a robust control environment, allow for audits, limit access to key functions to specified users, and be able to reconcile with other internal and external data.

WAY FORWARD FOR DIGITAL READINESS

The AI based surveillance mechanism and framework leverages all the digital capabilities of the organization and offers a robust and scalable framework where data driven and culture building practices provide a holistic environment that leads to a secure framework and mitigates operational risk, especially led by rogue trading and other off trading practices. Putting a structured framework works as a significantly effective deterrent against ongoing cyber and internal attacks and compromising positions for the organizations. Since this is a dynamic and never ending process, it is essential that organizations should align dedicated teams on research and analysis of other possible scenarios and enrich surveillance index organically and inorganically. There is also a need to view actions taken by RPA-led engine and review the performance in pre and post implementation conditions. Assessment of risk requires innovative ways of measuring risk - be it interviews, suggestion system, floor governance and secondary data inputs which is from the qualitative point of view and not covered in the present way of working. Big data based analysis covering both unstructured and structured data offers intelligent monitoring of transactions and defined process which provide an opportunity to install early warning signals, lead indicators, caveats, advisories to seek vulnerable tendencies. Benchmarking and digital performance management standards too need to be developed in this space, which may also prove useful in leveraging digital capability for business performance.

ABOUT THE AUTHOR

NEERAJ PARASHAR is Practice Head of BFS, Global Risk & Compliance, Digital and Design Lab for Tech Mahindra, and has also worked as Global DPO for TechM. He is pursuing PhD in Digital Transformation (where he has written digital performance management standards), and MBA (Information Systems and Marketing) from IMS, Indore, M.Phil. in Economics, Certified DPO, Six Sigma MBB, Lean Master, PMP, CIO Said-Garter Certified Professional and an alumnus (Diploma in Software Engineering) of Carnegie University of Pittsburgh, USA. With over 18 years of experience in consulting (operational, architecture and advisory) and managing delivery of Digital and RPA based organization excellence projects i.e. focusing IT and business outcomes especially in the domains of telecom, banking, financial services and insurance. He has managed client engagements in RSA, Singapore, India, UK, EU and US. The solutions developed by Neeraj have benefited customers not only in seeking financial impacts but also in effectively deploying digital business strategic capabilities.