CAPCO

THE FUTURE OF SURVEILLANCE & MONITORING

EMERGING PRACTICES

a wipro company

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

Global Regulators are continually increasing pressure on financial institutions (FIs) to strengthen surveillance and monitoring detection, recognizing the links between different financial crime risks e.g., fraud, money laundering, trade surveillance and demanding faster identification of financial crime risk. The pandemic has also seen significant increases in fraud volume and proliferation of new money laundering techniques. All this has presented opportunities for bad actors to exploit criminal opportunities in digital channels.

This requires FIs to rethink the way they prevent, detect, and monitor suspicious activities across different financial crime threats. Those FIs that transition to a Future model of surveillance and monitoring can create a competitive advantage by focusing on key risks to increase the return on investment and get the balance right into managing the risks in the specific areas the business wants to grow. This paper explores a potential path going forward and the benefits and the challenges of this new model of surveillance and monitoring.

Effective surveillance and monitoring require the following:

- Prioritize efforts on a risk-based approach – identify your key risks and control gaps using an integrated risk assessment and control framework
- Monitor activity on an ongoing basis
- Integrate data sources across the organization
- Use Artificial Intelligence and Machine Learning for screening and monitoring transactions
- Use Enterprise Case Management (ECM) tool to consume alerts from disparate systems

The key drivers for change include:

- complex expectations from global regulators,
- continuous controls and risk monitoring,
- a rapidly evolving criminal landscape,
- increased customer expectations and
- a drive to reduce operational and organizational costs.

2. BACKGROUND AND CONTEXT

A recent speech by the FCA at a Financial Crime summit highlights[1] the evolving complexity and sophistication of the criminal threat and the need to develop a whole system response, with firms and external agencies sharing intelligence and quickly responding to a constantly changing landscape.

Recent guidance also emphasises the challenges and expectations of regulators, as an example the FCA's thematic review[2] on Understanding the Money Laundering risks in the Capital Markets highlighted that many FIs mainly focused on detecting market abuse, however they ignored the potential link to associated money-laundering suspicions, "The risk that money-laundering threats and vulnerabilities are not considered is increased where market-abuse surveillance teams and functions sit in isolation, or even in different jurisdictions, from their AML colleagues".

FINCEN and the FCA are both championing technology innovation, with a key component of the United States reform of the BSA / AML via Anti-Money Laundering Act of 2020[3] being the exploration and adoption of new technologies to combat financial crime and other illicit activities more effectively.

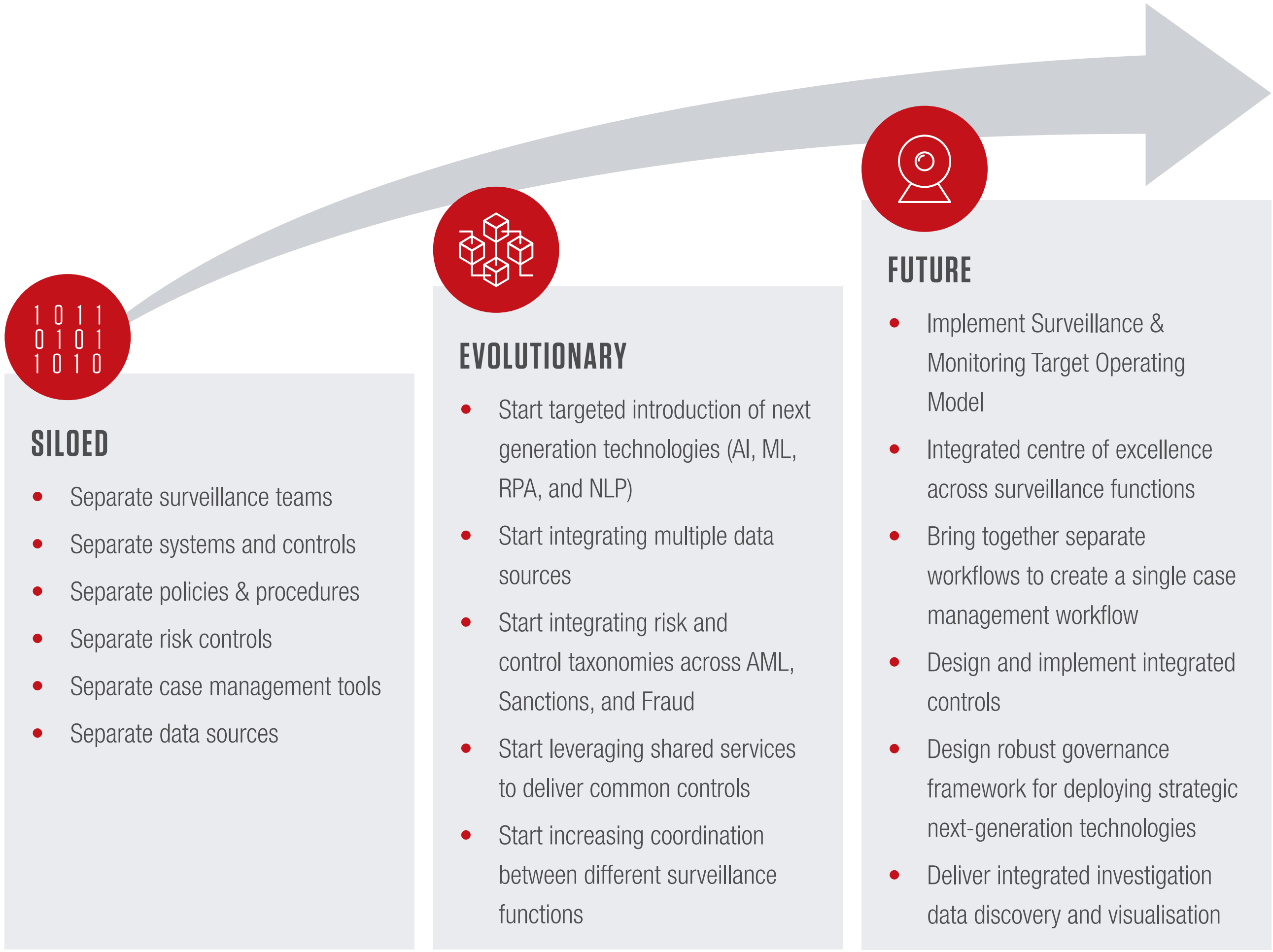
The FCA talks about its desire to become a "digital regulator" and its focus on fostering innovation, being intelligence-led and preparing for the future. An example of this focus is the FCA and Payment Systems Regulators (PSR) hosting of an Authorised Push Payment Fraud Tech Sprint (September 2022)[4] to work with industry to explore technology solutions that could be used to combat these types of Fraud.

These increased Regulatory expectations are driving FIs to enhance and more effectively leverage surveillance and monitoring detection, recognizing the links between different financial crime risks and market abuse, combined with an expectation of faster identification and management of these threats.

As the focus and expectation of regulators as well as the associated operational challenges increase, there is an opportunity to move away from the current siloed approach to identifying and managing Financial Crime and Market abuse risk.

Future Surveillance is the target state of a transformational journey to better detect and monitor interconnected threats (AML, Sanctions, Fraud and Trade Surveillance) by combining a wider set of data sources with advanced data analytics to build a comprehensive picture of the risk presented across the organisation, this improved visibility and connectivity, delivers enhanced risk management and operational efficiencies.

We propose a phased approach to transition from the 'siloed' financial crime operating model to an 'evolutionary' model before reaching a 'future' model.



SILOED

- Separate surveillance teams
- Separate systems and controls
- Separate policies & procedures
- Separate risk controls
- Separate case management tools
- Separate data sources

EVOLUTIONARY

- Start targeted introduction of next generation technologies (AI, ML, RPA, and NLP)
- Start integrating multiple data sources
- Start integrating risk and control taxonomies across AML, Sanctions, and Fraud
- Start leveraging shared services to deliver common controls
- Start increasing coordination between different surveillance functions

FUTURE

- Implement Surveillance & Monitoring Target Operating Model
- Integrated centre of excellence across surveillance functions
- Bring together separate workflows to create a single case management workflow
- Design and implement integrated controls
- Design robust governance framework for deploying strategic next-generation technologies
- Deliver integrated investigation data discovery and visualisation

Figure 1 – Key steps of transformation journey

3. A SILOED APPROACH TO SURVEILLANCE AND MONITORING

Financial institutions with a siloed approach to the detection and monitoring of financial crime and market abuse run the risk of missing the potential correlation and interconnections between the different threats across fraud, money laundering, sanctions, and trade surveillance. The current siloed approach is illustrated in Figure 2.

In general, transaction monitoring, fraud detection, sanction screening and KYC etc are currently managed by separate teams and case managers across different business lines and geographies. This is reflected by the supporting technology, most platforms are built upon a legacy technology infrastructure, with siloed data sources for multiple channels (and limited data synchronisation across platforms) and batched data processing . This along with a heavy reliance on manual activities (such as alert review, information searching among multiple source systems, investigation, escalation, QA/QC, and threshold tuning), results in a time and resource heavy activity.

Such a siloed approach has inevitably generated a variety of struggles within FIs:

- **Increased challenges in identifying threats:** a convergence of different forms of financial crimes and communication channels have led to increased challenges in identifying threats: isolated views of financial crime risks, investigation by separate teams, all limit the opportunities to identify and prevent inter-connected threats.

- **Exacerbated cost pressure:** funding is managed inefficiently, supporting multiple teams, systems and siloed architectures across different businesses and geographies, which exacerbated the significant cost pressures that FIs have already been facing.

- **Increased volume of false positive alerts:** Siloed data sources across multiple channels, batch processes and a heavy reliance on manual activities leads to a high number of false positive alerts, due to (1) suboptimal threshold values and lack of dynamic tuning under the siloed rules-based controls, and (2) data quality issues/data mismatching across multiple systems. Investigation of these unproductive alerts cost a large amount of time and resource, resulting in operational bottlenecks and leading to low alert to suspicious-activity-reporting (SAR) ratios.

- **Delayed alerts:** surveillance and monitoring data are usually fed and processed in batched process, rather than in a real time mode, which can hinder the timely discovery of potential Financial Crimes.

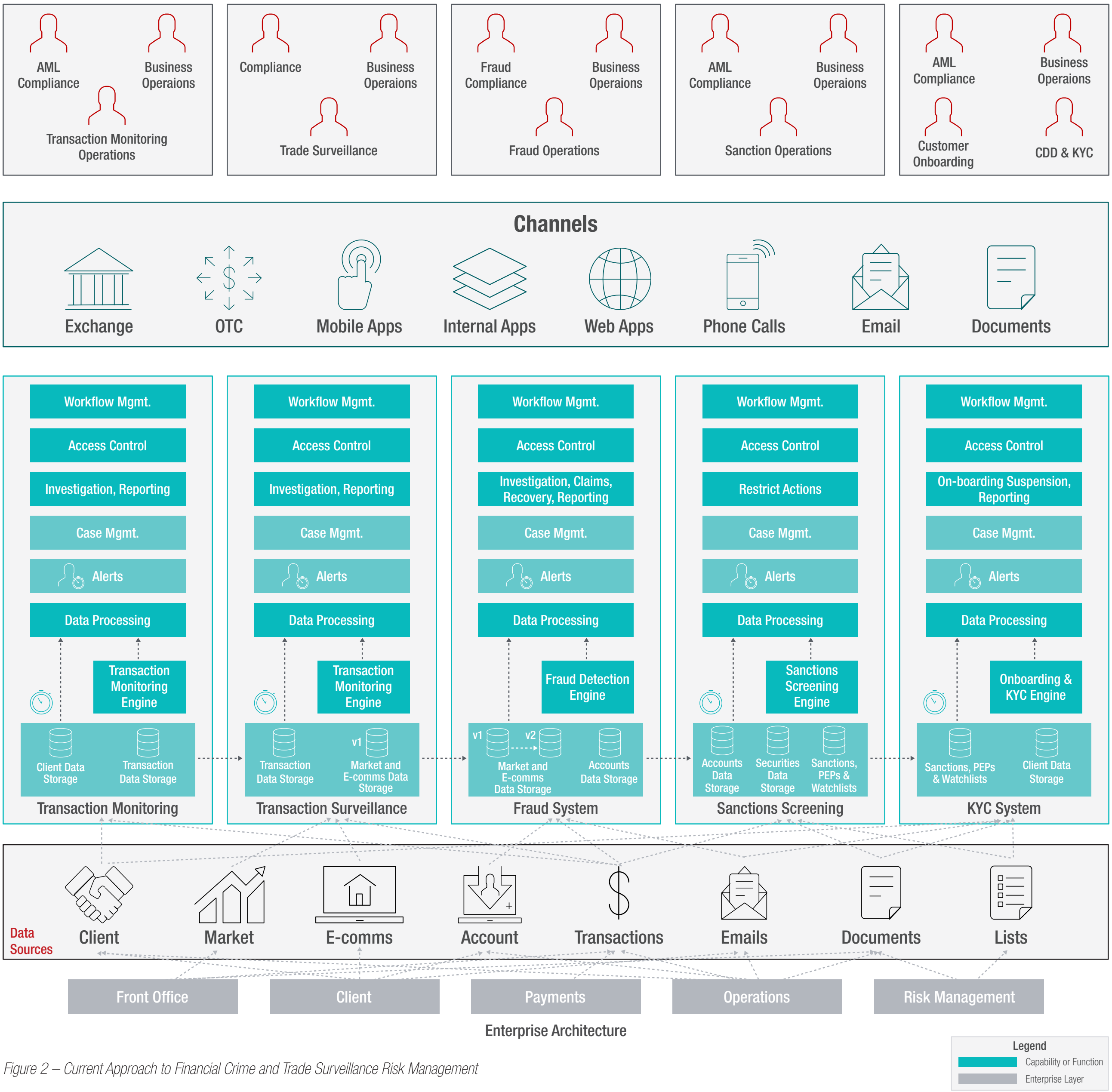


Figure 2 – Current Approach to Financial Crime and Trade Surveillance Risk Management

4. THE EVOLUTION TO A FUTURE SURVEILLANCE AND MONITORING FUNCTION

The traditional financial crime model involves many disparate policies, procedures, systems, and data sources operating in silos across teams with limited centralized data management and opportunities to generate interconnected insights. As financial crime becomes more sophisticated this model provides little flexibility to scale and becomes more and more complex leading to increasing costs and reduced effectiveness. Change is required, but at what cost?

The transition to Future Surveillance & Monitoring is a complex, multi-year journey involving more than Technology change. Financial crime policies and processes will be re-designed and where applicable, digitised. Essential to the journey will be business, operational and organizational model changes that merge and simplify surveillance and monitoring functions around a Surveillance & Monitoring Centre of Excellence (CoE). In the transition, the CoE validates the pre-defined outcomes prior to scaling solutions across different risk typologies of the monitoring capability. Ultimately, formation of a CoE can effectively reduce the number of case managers and enable efficient communications between Financial Crime Defence teams (e.g., AML compliance, Business Operations, Transaction Monitoring Operations etc, shown in Figure 3), and thus identification and prevention of inter-connected Financial Crimes.

A Future State Technology architecture to support this change is illustrated in Figure 3.

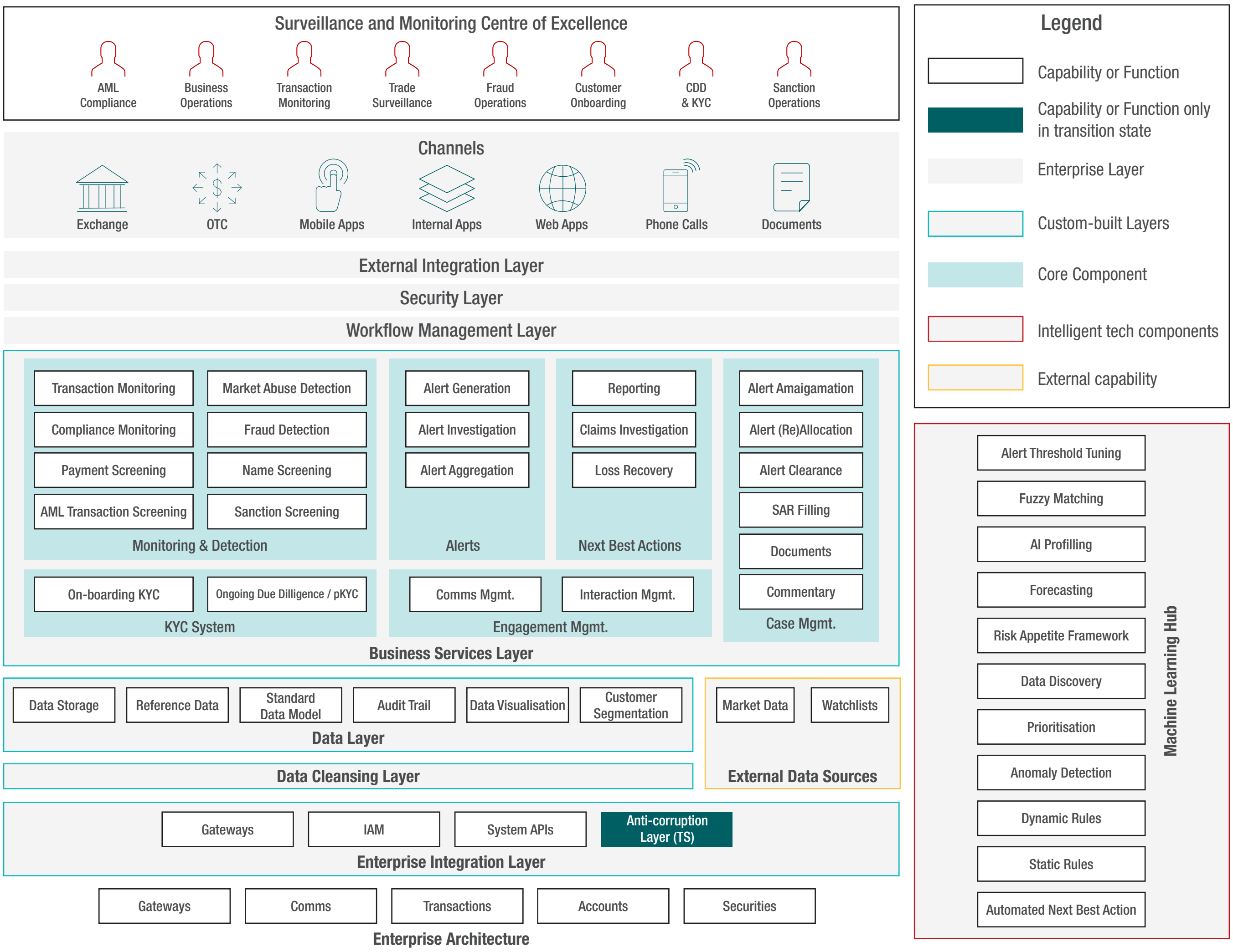


Figure 3 – Future surveillance & Monitoring: Target state architecture example

As shown above, the key technical changes for FIs looking to move to a future surveillance & monitoring technology architecture would involve:

- Introducing an **Enterprise Integration Layer,** to enable access to internal systems via APIs.
- Creating a **Data Cleansing Layer** and integrated **Data Layer,** with a standardized data model, providing an integrated view of risk, across Financial Crime, Sanctions, Fraud and Market Abuse.
- Designing a **Business Service Layer,** to replace siloed and duplicated functions to provide core functions and capabilities. Particularly, an enterprise **Case Management** service is key, to ingest and enhance alerts generated from existing monitoring systems and group and prioritize alerts for investigation;
- Creating a **Machine Learning Hub** to reduce manual processes, with the introduction of advanced analytics and intelligent automation throughout the Business Services Layer. Joining together the power of machine learning with dynamic rule setting alongside a combined data layer, generation of false positive alerts (due to data mismatches and rule setting) can be effecitively reduced;
- Introducing a **Workflow Management Layer,** to define and execute flows of activities or tasks, either as an audited, manual set of activities or in response to automated events.

5. BENEFITS OF UPSCALING SURVEILLANCE AND MONITORING

Whilst transformation of this nature comes with challenges, the adoption of Future surveillance can bring multiple benefits provided that the solution has been tailored to the Financial Institution and it's tactical and strategic drivers.

Enable business strategy: Create a competitive advantage and increase revenue through use of intelligence led monitoring allowing the business to market new products, expand to new geographies and attract new customers

Reduce Costs: Merging siloed surveillance teams, technology rationalization, cost of controls management and leveraging the Centre of Excellence can provide consolidation benefits. Cost reductions can also be realised due to the reduction in 'false positive' alerts leading to a more efficient use of investigator time, focusing work on alerts that pose a true risk to the organization.

Improve Risk Mitigation: Through more effective management of overall financial crime threat exposure, due to strengthened monitoring and detection capabilities, and a better view of the concentrated risk areas within the organization. Risk mitigation can also be obtained through improving the set of controls in place, enabling better detection of financial crime risk in a way that is complete and more accurate.

6. NEXT STEPS FOR IMPLEMENTING THE FUTURE SURVEILLANCE & MONITORING TECHNOLOGY ARCHITECTURE

Transitioning from the current siloed approach to a future target state requires careful planning and several transition states. The below section outlines high level next steps to transition successfully.

Before transitioning, organisations should ask themselves "What can we move to the cloud?"

FIs should assess the current state of their platform architecture and analyse the feasibility of cloud migration. This includes identifying the potential impact of cloud migration on the stakeholders, as well as potential risks during the transition phase, whilst setting up strategies for mitigating negative impacts and risks.

Transition Phase 1: Focus on a unified data model and build the Enterprise Integration Layer

The first task is to begin to integrate multiple data sources against a common data model to help understand the overall financial crime risk. Then FIs can build out a centralized, integrated data architecture connected by an Enterprise Integration Layer and a temporary layer following the Anti Corruption Layer pattern to ensure that the transition is undertaken with a reduced risk.

Transition Phase 2: Build the business service layer and integrate the Machine Learning Hub:

In this transition phase, FIs start to move applications from the existing Enterprise Architecture to the Business Services Layer in iterative, functional steps and slowly eliminate applications that do not offer unique capabilities. Alongside this work a machine learning hub should also be built to maximise benefit from the business service layer using the latest technologies.

Target state: Retire the ACL:

Once all functionality that can be migrated has been re-architected as functional services within the business layer, remove the temporary integration layer (the Anti-corruption Layer), and use System APIs as the integration point throughout subsequent transitioning process.

7. CHALLENGES FOR FIS IMPLEMENTING THE FUTURE SURVEILLANCE & MONITORING MODEL

Transitioning to the Future Surveillance & Monitoring model is not a simple process and presents several challenges.

Data & Technology Challenges: Inconsistent data models make data aggregation and data discovery at a customer and entity level difficult.

Data quality is particularly important during the journey as it could be an obstacle to the adoption of advanced analytics using Machine Learning (ML) techniques. Additionally, supervision, transparency and explainability of the applied intelligent techniques (e.g. AI/ML) also needs to be addressed.

As for the technology architecture, current fragmented financial crime systems based on legacy technology platforms could limit the ability to standardize and integrate into a common platform.

Risk and Regulatory Challenges:

Integration of data sources might also result in exposure of data to new business or technology functions and therefore introduce further regulatory requirements. For example, certain data may be migrated from on-prem databases to cloud platforms; therefore, data governance and regulatory compliance will also need to be addressed throughout this process.

Management & Operational Challenges:

Gaining senior management commitment to move to an integrated financial crime risk management approach may take some time.

Siloed organisational structures (e.g., AML, market abuse, sanctions, fraud) can hinder the management of financial crime risk across the whole FI. Therefore, there could be additional requirement for re-designing organisational structures (and also ways of working).

8. HOW CAN CAPCO HELP FINANCIAL INSTITUTIONS IN THEIR SURVEILLANCE AND MONITORING TRANSFORMATION JOURNEY

Capco's dedicated Financial Crime experts, working alongside our technology and data capability deliver solutions and insights leveraging next generation technology, investing with clients to build custom solutions for solving complex problems.

We define and execute end-to-end solutions and have capabilities across multiple locations to support your needs including on-site services, near-shore, and off-shore, along with tools and accelerators being applied at multiple clients as well as supporting financial crime as a Managed Service.

Capco's expertise in the evolution of monitoring and surveillance include:

- Operating Model Design & Implementation
- Data Quality Management
- Data Analytics & Optimisation
- Technology Architecture & Implementation
- Processes And Controls

Speak to us if you want to learn more.

9. BIBLIOGRAPHY

1. Fighting financial crime – the force multiplier effect. **Financial Conduct Authority.** s.l. : https://www.fca.org.uk/news/speeches/fighting-financial-crime-force-multiplier-effect, 2022

2. **Financial Conduct Authority.** FCA TR19/4. TR19/4: Understanding the money laundering risks in the capital markets. [Online] 10 06 2019. https://www.fca.org.uk/publications/thematic-reviews/tr19-4-understanding-money-laundering-risks-capital-markets

3. **The Anti-Money Laundering Act of 2020.** U..S. Financial Crimes Enforcement Network. [Online] 30 June 2021. https://www.fincen.gov/anti-money-laundering-act-2020

4. **Authorised Push Payment Fraud TechSprint.** UK Financial Conduct Authority. [Online] 2022. https://www.fca.org.uk/events/authorised-push-payment-fraud-techsprint

AUTHORS

David Leftley, Senior Consultant
Jessica Bevan, Senior Consultant
Ziyi Liu, Associate

CONTACTS

David Cecil, Managing Principal
david.cecil@capco.com

Dimitris Vougiouklis, Managing Principal
dimitris.vougiouklis@capco.com

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy specializing in driving digital transformation in the financial services industry. With a growing client portfolio comprising of over 100 global organizations, Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to deliver end-to-end data-driven solutions and fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its Innovation Labs and award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on Twitter, Facebook, YouTube, LinkedIn Instagram, and Xing.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

JN_4693