OLIVER WYMAN

EFFICIENT AND EFFECTIVE FINANCIAL CRIME COMPLIANCE

DISPELLING THREE COMMON MYTHS TO ENABLE NEXT GENERATION SOLUTIONS

EFFICIENT AND EFFECTIVE FINANCIAL CRIME COMPLIANCE: DISPELLING THREE COMMON MYTHS TO ENABLE NEXT GENERATION SOLUTIONS

Banks globally spend more than $12 billion a year and employ many tens of thousands of people on financial crime compliance (FCC), covering Anti-Money Laundering (AML) and Sanctions & Embargoes regulations. One would hope that such a large investment has allowed banks to most effectively identify and report on suspicious activity. This, unfortunately, is not the case, and frustrations with current industry solutions are widespread.

There is, however, a real opportunity to improve performance and reduce costs by moving to the next generation of solutions. These include automation of routine tasks, better data and enhanced analytical models, streamlined organization and governance, and improvements to the overall operating model. We have already seen some banks reap considerable benefits from the first steps in this direction. To seize the opportunity fully, banks need to think about the problem on an end-to-end basis, rather than by operating in silos or through discrete technical solutions.

Those that successfully embrace next generation FCC/AML solutions will reap multiple benefits:

- More accurate identification of suspicious activity and better response to requests from law enforcement
- Lower costs and greater effectiveness by eliminating false positives and optimizing often manual investigation processes
- Higher customer satisfaction and increased revenue by streamlining client onboarding and product approval processes, facilitating rapid and secure transaction approval, and avoiding unnecessary de-risking
- More rapid and comprehensive response to new regulatory requirements

These benefits will allow the FCC/AML function, and the lines of business they support, to focus on higher-value activities as routine work is automated and supported by better data and improved analytical models.

There is potential for large and sustainable improvement. However, the journey will not be easy. To undertake this journey, banks will need to confront a number of commonly held myths:

Myth 1: FCC/AML solutions involve a tradeoff between efficiency (doing things cheaper) and effectiveness (doing things better)

Reality:

- Next generation solutions are both more efficient and more effective than current approaches. It is possible not only to reduce costs but at the same time to improve risk coverage and risk mitigation while not pushing the boundary too much in terms of complexity of solution.
- One of the biggest challenges is to achieve regulatory compliance rather than improve performance. Next generation solutions can increase resiliency to change, providing flexibility to respond to future regulatory imperatives, and importantly provide more useful inputs to law enforcement in the fight against financial crime.

Myth 2: Next generation FCC/AML solutions rely solely on dynamic machine learning (ML) and artificial intelligence (AI) type applications

Reality:

- There is a big opportunity to drive significant impact for next generation FCC/AML solutions through a range of levers, for which ML and AI lie at the more sophisticated end. Banks should first exhaust "lower hanging fruit" and subsequently take care of where, when, and how they apply dynamic ML and AI.

- Making impactful, if less sophisticated, changes that create traction within the organization and meet regulatory expectations is worth far more than theoretically effective changes that do not gain acceptance. This does not mean there are not ways to use more sophisticated techniques such as ML and AI, but there are a lot of worthwhile improvements that do not rely on these.

Myth 3: Individual proofs of concepts (POCs) are sufficient to drive a step change in overall system performance

Reality:

- While individual POCs can solve specific problems they are not sufficient on their own to drive transformation. They may produce headline results, but are often not sustainable or scalable without considering the broader ecosystem. Banks need to take a much more strategic and transformative approach to unlock the full potential value.
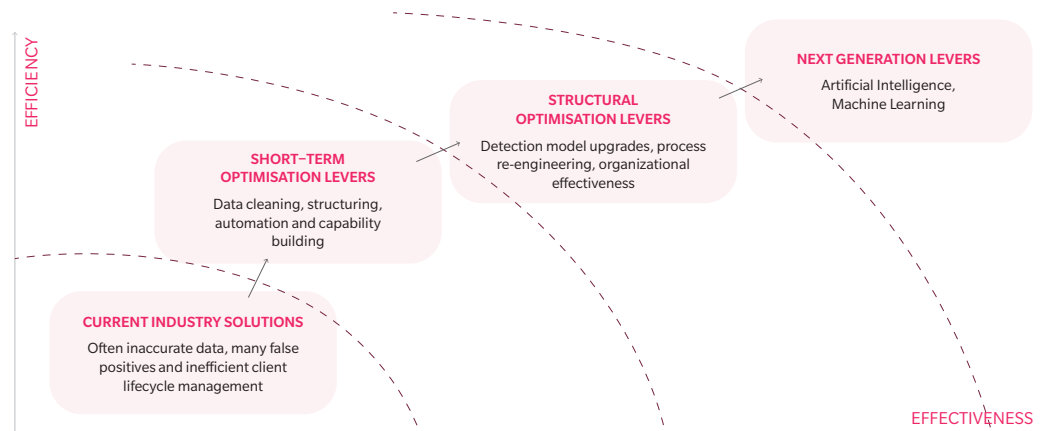
- The prioritization and timing of initiatives is critical to ensure success. This requires a top-down view of risk and performance to understand the potential impact and optimal sequencing of initiatives to drive sustainable improvements on an end-to-end basis.

The illustration below lays out a path for improving efficiency and effectiveness. (See Exhibit 1). It deploys a sequence of initiatives of increasing sophistication to realize shorter term opportunities, drive structural optimization changes, and ultimately enable next generation solutions.

In this point of view, we proceed as follows:

- First, we assess each of these myths in turn and explore their implications for banks

- Second, we lay out a strategic FCC/AML framework for next-generation solutions

- Third, we outline challenges to be overcome and approaches to them

Exhibit 1: Impact of different groups of optimization levers on effectiveness and efficiency (not exhaustive)

EFFICIENCY

EFFECTIVENESS

NEXT GENERATION LEVERS
Artificial Intelligence, Machine Learning

STRUCTURAL OPTIMISATION LEVERS
Detection model upgrades, process re-engineering, organizational effectiveness

SHORT-TERM OPTIMISATION LEVERS
Data cleaning, structuring, automation and capability building

CURRENT INDUSTRY SOLUTIONS
Often inaccurate data, many false positives and inefficient client lifecycle management

- Finally, we look at how banks should move forward and the benefits of doing so

Addressing Myth #1:

How can banks be confident that the adoption of next generation solutions will not involve a tradeoff between efficiency and effectiveness and what are the implications of this?

This point may be argued through a theoretical examination of current industry solutions and their key strengths and weaknesses. However, we believe it is easier to substantiate through some real-life examples.

The first example (see below) looks at how banks may drive significant improvements in detection models. In this case for transaction monitoring, there is not only a reduction in the number of false positives, but also an increase in the number of quality SARs reported.

The second example looks at how banks may drive significant improvements in process. In this case for client onboarding/KYC, it can

	REAL LIFE EXAMPLE #1: ADVANCED TRANSACTION MONITORING RISK SCORE	REAL LIFE EXAMPLE #2: REENGINEERING OF CLIENT ONBOARDING / KYC
Situation	Large US bank using industry standard transaction monitoring system Large number of false positives generated by traditional Transaction Monitoring (TM) analytical models, the analysis of which required significant time and resources Large numbers of criteria (more than 100) within scenarios for case generation, which was costly and difficult to maintain and update	Leading emerging markets bank with traditional RM sales and client service in commercial segment Long and comprehensive procedures on how to perform KYC, but not written from an efficiency perspective Duplication in collection of information at multiple points in the KYC/ onboarding process and multiple points of rework both at client interface and internally
Approach	Introduced an advanced transaction monitoring risk score to reduce false positives and increase number of quality SARs reported Performed detailed model design to define key modelling choices including target variable(s), data perimeter, development window, periodicity, sample size and sampling approach, and implementation options Performed sample collection including above-the-line and below-the-line alerts to support model development Developed a number of alternative candidate models to allow tradeoff of performance improvements vs. model complexity and regulatory acceptability Tested and implemented new model	Introduced a matrix to clearly define documentation required to perform KYC for different clients and products Redesigned the application forms for current accounts and simple and standard credit products Increased use of electronic verification and automated checks and reduced duplicative manual controls Introduced new streamlined utility back office for accounts requiring referral Trained the RMs to request the right documents from the client first time in the majority of cases Implemented 25+ individual IT fixes to pre-populate information already available and eliminate double entry across KYC, onboarding and credit systems
Impact	Reduction of 20% to 40% in false positive ratio (depending on the scenario) 30%+ reduction in number of criteria making models easier to maintain and update 10% increase in number of quality SARs reported	Reduction of more than 20% of direct non-sales costs for account opening Reduction of more than 30% in time for client to open current account product and between 40% and 50% for client to open standard credit product Increase of more than 40% in commercial time available for RM

be observed that not only is there a reduction in cost, but also in the client onboarding time and an increase in the productive time available for the relationship manager (RM).

The fact that next-generation solutions improve both efficiency and effectiveness makes for a much more compelling regulatory narrative, which is critical. In addition, reducing the burden and time to decision for customers, and improving the productivity of commercial facing staff makes the transformation case much easier to argue to internal stakeholders of the bank.

Addressing Myth #2:
If next generation FCC / AML solutions do not need to rely on dynamic machine learning (ML) and artificial intelligence (AI), how should banks proceed?

There are multiple levers and improvement opportunities that may impact FCC/AML risk management, FCC/AML operations, and the business lines. The table overleaf lays out some examples that may be used to drive significant improvements in performance.

We do see a role for ML and AI within this range of levers. However, they are often not the first levers that should be pulled, and do not obviate the need for a proper detailed understanding of the specific problems and issues at hand. We argue that banks need to be careful **where**, **when**, and **how** they apply dynamic ML and AI techniques.

Where: ML and AI are not "silver bullets" that will magically solve all issues across the FCC / AML lifecycle. Therefore, careful thought needs to be given on where to best apply these techniques. For example:

- The level of regulatory scrutiny will rightly be much greater if ML or AI is applied as a mechanism to reduce false positives in the alert generation process prior to human intervention and review.

- However, if ML and AI are applied in the detection of false negatives or as part of the investigative process to support and enhance subsequent human review, there is likely to be much less resistance.

When: Institutions should make sure that they have first exhausted lower hanging fruit and have the required level of analytical sophistication before they focus on ML and AI. For example:

- If investigators are manually sourcing and copying and pasting data from multiple disparate sources, it makes sense to structure and automate this first before moving to ML and AI.

- If key stakeholders are not sufficiently informed or do not have the required resources and skillsets to support more advanced analytical techniques, it does not make sense to race too far ahead to introduce sophisticated ML and AI that will not get traction.

How: It is not sufficient to apply these techniques as "black box" solutions. There must be sufficient transparency in the process and the outcomes produced, commensurate with the proposed application.

- In our view, it is not desirable to apply these techniques in the absence of well-established model development and model risk management standards that govern their development, validation, monitoring, and use; in many institutions, such standards are still at an emerging stage.

- One option is the production of a series of candidate models that trade off model complexity and performance against transparency and regulatory acceptability; this will allow the institution to demonstrate a spectrum in sophistication of solutions and be judicious in selection of a model

Exhibit 2: Select examples of levers and improvement opportunities (not exhaustive)[1]

AREA	SELECT LEVERS AND IMPROVEMENT OPPORTUNITIES
Models	Improving data quality, enhancing the data perimeter, and improving data connectivity will reduce noise, allow unexpected cash-flows to be better explained, and reduce the need for manual human intervention Improving the granularity and behavioral elements of segmentations will allow more accurate identification of specific clients such that rules and thresholds are calibrated on the basis of expected outcomes and specific risks rather than on a broad-brush basis Fully leveraging well-established statistical techniques will facilitate more dynamic parameterization and capture nonlinear interactions providing significant uplift that may be much easier to explain to regulators than AI or ML
Processes	Introducing well-structured, business-orientated procedures will ensure that specific clients and transactions are treated appropriately, given their complexity and risk and improve the efficiency of investigative work Reengineering processes to pre-populate data inputs from existing data sources, eliminate duplication in activities, and introduce automated controls will reduce time spent on manual activities, eliminate rework, and improve quality control Strengthening linkages and putting in place strong feedback loops will improve effectiveness, for example by ensuring that all relevant KYC information is fully leveraged in transaction monitoring, and ensuring that all relevant transactional information is fully leveraged in KYC renewals Introducing well-structured but dynamic output templates will help to ensure that the right information is presented at the right time to the right audience, ensuring that human time is spent on the most relevant and value adding activities
Governance and Organization	Putting in place strong governance will ensure senior management is working together effectively at the interface of regions, business lines, and risks types (such as AML, sanctions, and fraud) Performing a staffing assessment to understanding the overall staffing requirements and skillset of individuals will allow the organization to be right-sized and up-skilled Ensuring that training is pragmatic and deals with the specific skillset required for the particular role will make people more effective
Operating Model	Clarifying roles between lines of defense (such as operations vs. risk management) and creating centers of excellence will remove duplication, driving specialization where required while promoting cross pollination and skills development Balancing regional/divisional responsibilities to standardize functions where possible and ruthlessly evaluating oversight needed locally vs. centrally will help to effectively balance control and flexibility Defining and baselining specific, pragmatic, and objective risk tolerance across client/product profile, controls, and outcomes (for example, "what is an acceptable level QA for KYC?" or "how many customers with multiple SARs are we willing to bank?") will support decision making and resource allocation Putting in place effective dashboards will facilitate an understanding of performance on an end-to-end basis, drilling down to the individual level and highlighting bottlenecks and improvement opportunities Embedding tolerances and goals into performance scorecards will improve transparency and accountability

1 For additional discussion on FCC operating models, see www.oliverwyman.com/our-expertise/insights/2018/jul/financial-crime-risk-management-in-asia-pacific.html and www.oliverwyman.com/our-expertise/insights/2018/jul/financial-crime-risk-management-in-australia.html.

that improves performance but does not push the boundaries too far.

ML and AI may not always result in substantial and sustainable improvements in performance and may in reality be much more difficult to explain and justify to regulators. By adopting a more nuanced and sequential approach, banks can still capture significant uplift and gain regulatory buy-in along the way as they progress towards more sophisticated solutions. (See Exhibit 3).

Addressing Myth #3:
If it is not possible to unlock the full potential of next generation solutions through individual proof of concepts (POCs), how should banks proceed?

Individual FCC/AML solutions are often developed to solve very specific issues: provide the first line of defense with better intelligence about their customer base, build an improved risk score to reduce transaction monitoring false positive rates, reengineer document collection, and review for customer onboarding to reduce reliance on manual intervention. These individual solutions can often deliver on their stated objectives and effectively demonstrate the strength of individual concepts. However, without a strategic FCC/AML framework to support proper prioritization and link to enterprise standards, the overall effectiveness of next-generation solutions is at risk. Pilots developed in the absence of an overall strategic optimization framework may:

- Use bespoke techniques or approaches that are incompatible with other solutions and/or established standards, making it difficult to absorb into the enterprise (including risk appetite and measurement standards,

existing policy, previous regulatory communication, and IT standards)
- Fail to factor in data or validation standards, making it difficult to implement such solutions beyond proofs of concept
- Rely on a very specialized and focused team with a skillset not widely available in the main organization, preventing scalability
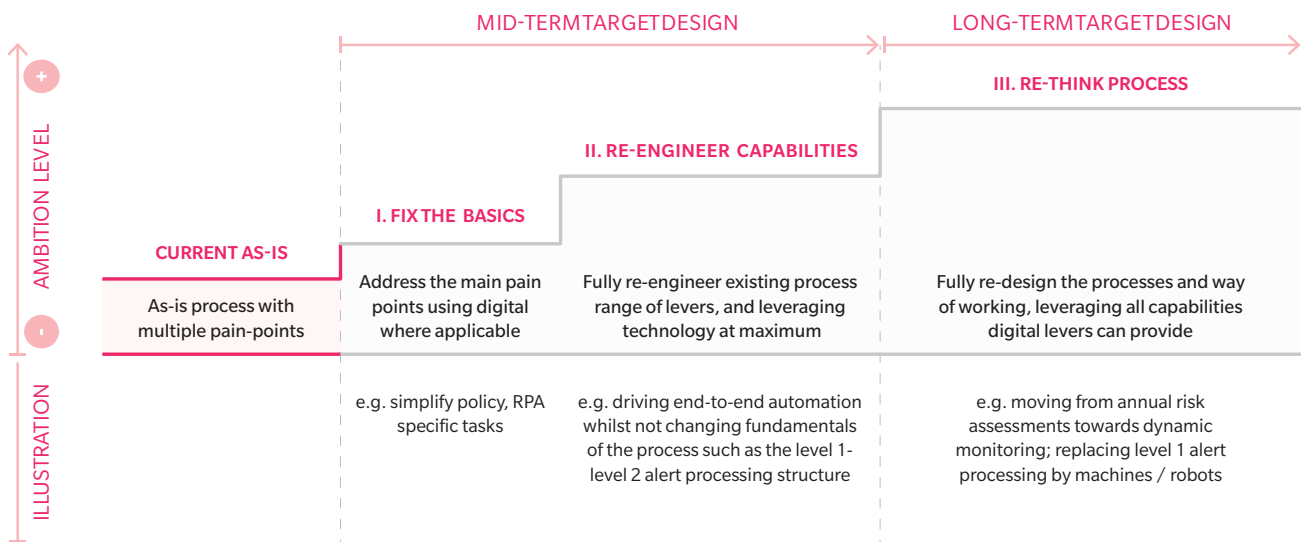
Establishing a strategic framework ensures that an individual solution development aligns with an organization's stated objectives, as well as other existing, in-flight, and planned initiatives. A strategic framework can also impose standards on pilots to ensure they do not get stuck in a POC phase with no clear path to fully embed in the organization.

Of course, effective solution generation and deployment requires balance and the provision of enough space to innovate. Piloting solutions through the development of a POC within a single business unit (or for a specific product or within a region) can establish whether an idea can be successfully deployed (as long as it complies with the bank's global standards). In fact, pilots can often refine solutions to help get them ready for prime time.
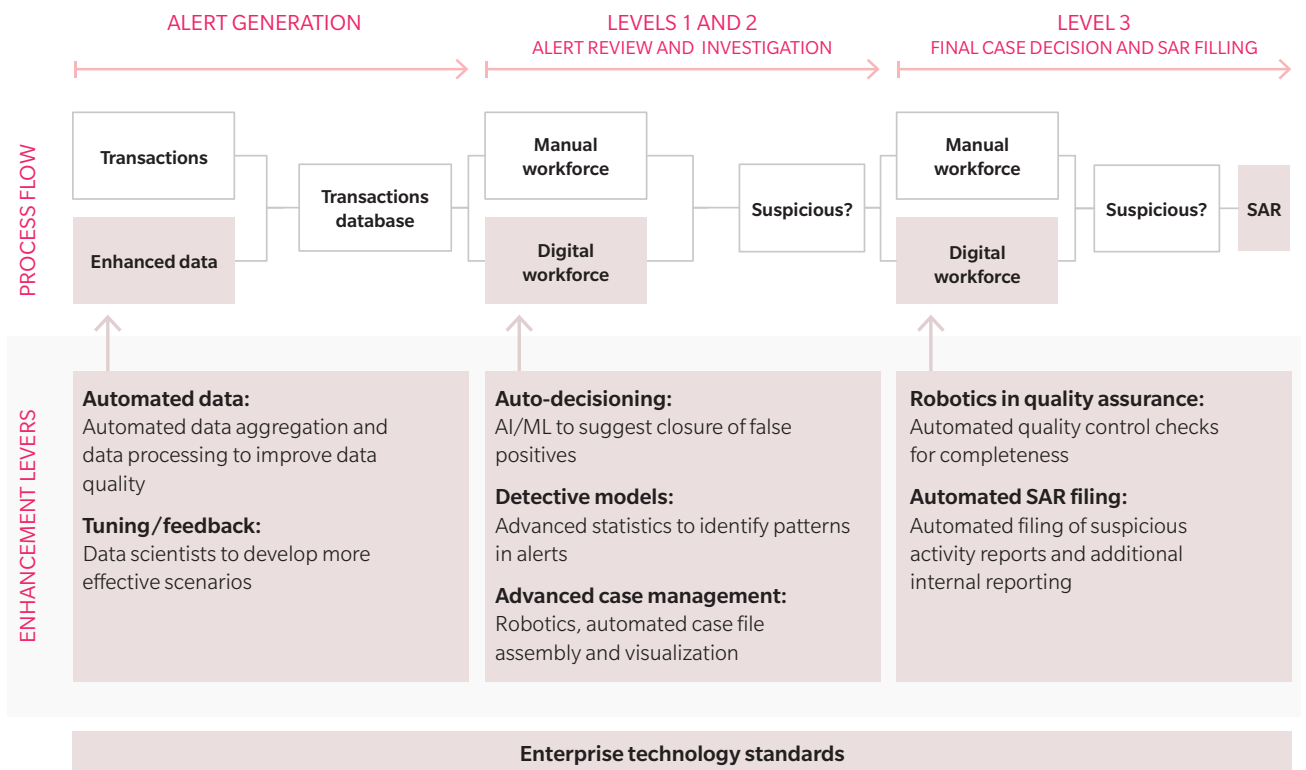
The example below looks at how a bank prioritized initiatives to improve transaction monitoring. (See Exhibit 4). Through an analysis of the end-to-end process, the specific issues at various points in the process, and an appreciation of global compliance and technology standards, the bank was able to drive impactful and sustainable change.

Exhibit 3: Practical application of optimization levers in FCC / AML process design

		MID-TERM TARGET DESIGN		LONG-TERM TARGET DESIGN

AMBITION LEVEL (+ to -)

	CURRENT AS-IS	I. FIX THE BASICS	II. RE-ENGINEER CAPABILITIES	III. RE-THINK PROCESS
	As-is process with multiple pain-points	Address the main pain points using digital where applicable	Fully re-engineer existing process range of levers, and leveraging technology at maximum	Fully re-design the processes and way of working, leveraging all capabilities digital levers can provide
ILLUSTRATION		e.g. simplify policy, RPA specific tasks	e.g. driving end-to-end automation whilst not changing fundamentals of the process such as the level 1-level 2 alert processing structure	e.g. moving from annual risk assessments towards dynamic monitoring; replacing level 1 alert processing by machines / robots

---

Real life example #3: Leveraging digital capabilities to boost end-to-end efficiency and effectiveness in transaction monitoring

ALERT GENERATION	LEVELS 1 AND 2 ALERT REVIEW AND INVESTIGATION	LEVEL 3 FINAL CASE DECISION AND SAR FILLING

PROCESS FLOW

Transactions / Enhanced data → Transactions database → Manual workforce / Digital workforce → Suspicious? → Manual workforce / Digital workforce → Suspicious? → SAR

ENHANCEMENT LEVERS

Automated data: Automated data aggregation and data processing to improve data quality	**Auto-decisioning:** AI/ML to suggest closure of false positives	**Robotics in quality assurance:** Automated quality control checks for completeness
Tuning/feedback: Data scientists to develop more effective scenarios	**Detective models:** Advanced statistics to identify patterns in alerts	**Automated SAR filing:** Automated filing of suspicious activity reports and additional internal reporting
	Advanced case management: Robotics, automated case file assembly and visualization	

Enterprise technology standards

A STRATEGIC FCC/ AML FRAMEWORK

To fully realize efficiency and effectiveness opportunities, FCC/AML initiatives similar to the ones outlined above should be developed within a broader strategic FCC/AML framework (See Exhibit 5). A strategic FCC/AML framework will guarantee that the right metrics are in place and that senior management has visibility across the entire program.

The first step in this process is to articulate the overall FCC/AML strategy. With so many products and new technologies available in the FCC/AML space, it is possible to pursue a large number of new initiatives in parallel. By establishing and agreeing on an overall strategy and the capabilities required to deliver the strategy, management can co-ordinate the overall effort and direct attention and investment towards the most impactful initiatives.

Additionally, a comprehensive FCC/AML strategy will ensure that the right capabilities are in place to support each initiative, such that they can move beyond POC to full scale transformation initiatives. It will promote optimization both within and across silos and avoid localized solutions that may not deliver the maximum overall value or be compatible with the overall FCC/AML framework. Importantly, it will guarantee that issues can be surfaced and quickly resolved at a senior level, and facilitate the sharing of best practices and lessons learned.

1. RISK APPETITE AND OBJECTIVE SETTING:

Many institutions operate without a clear, top-down vision or principles for their FCC/AML function. Strategies are more often responsive and remedial, designed to correct last year's problems, rather than anticipate next year's. They generally focus on satisfying regulatory and audit expectations, rather than being oriented towards detecting suspicious activity in the most effective manner. Next-generation solutions will include a clearly articulated risk appetite that is cascaded into clear risk-adjusted objectives to set targets and track performance and support prioritization of initiatives across the program. A well-operationalized risk appetite, supported by well-calibrated monitoring tools, will enable the business of the bank.

2. ORGANIZATION AND GOVERNANCE:

Organizational structures are often arranged in silos, leading to sub-optimal interaction between groups. This lack of collaboration makes it difficult to ensure that the dots are connected amongst regional, business aligned, risk type, and functional groups. Given teams may also have gaps in the business knowledge and technical skills necessary to detect and interpret sophisticated threats and typologies. In order to successfully deploy next generation solutions, organizations will need to break down these silos where possible, and ensure that the required skillset and disciplines are brought together; this includes including traditional FCC/AML risk management, operational and analytical skills, and new agile and digital development methods. To make this effective and efficient, leading banks are increasingly looking to leverage methodological and process synergies across the non-financial risk spectrum, including FCC/AML, Regulatory Compliance, Operational Risk and Cyber.

3. FCC/AML LIFECYCLE:

As we look across the FCC/AML lifecycle, we observe two significant challenges. The first challenge is how to accurately detect activity that represents higher risk, such that there is not undue noise caused by generating alerts in benign cases, and conversely that truly suspicious activity is not missed. The second challenge is how to investigate alerted cases in the most efficient and effective manner, such that all the right information is collated, and objective and consistent decisions are produced.

Existing detection models used in FCC/AML are often based on simple rules or models that do not fully leverage available data, more advanced statistical methods, or the latest technological advancements. Next-generation solutions will include a deeper, more strategic risk identification process to determine actual problematic scenarios, leverage data available from across the organization, introduce more granular and behavioral segmentations, and proactively embrace more advanced analytical techniques.

Exhibit 4: Strategic FCC/AML framework
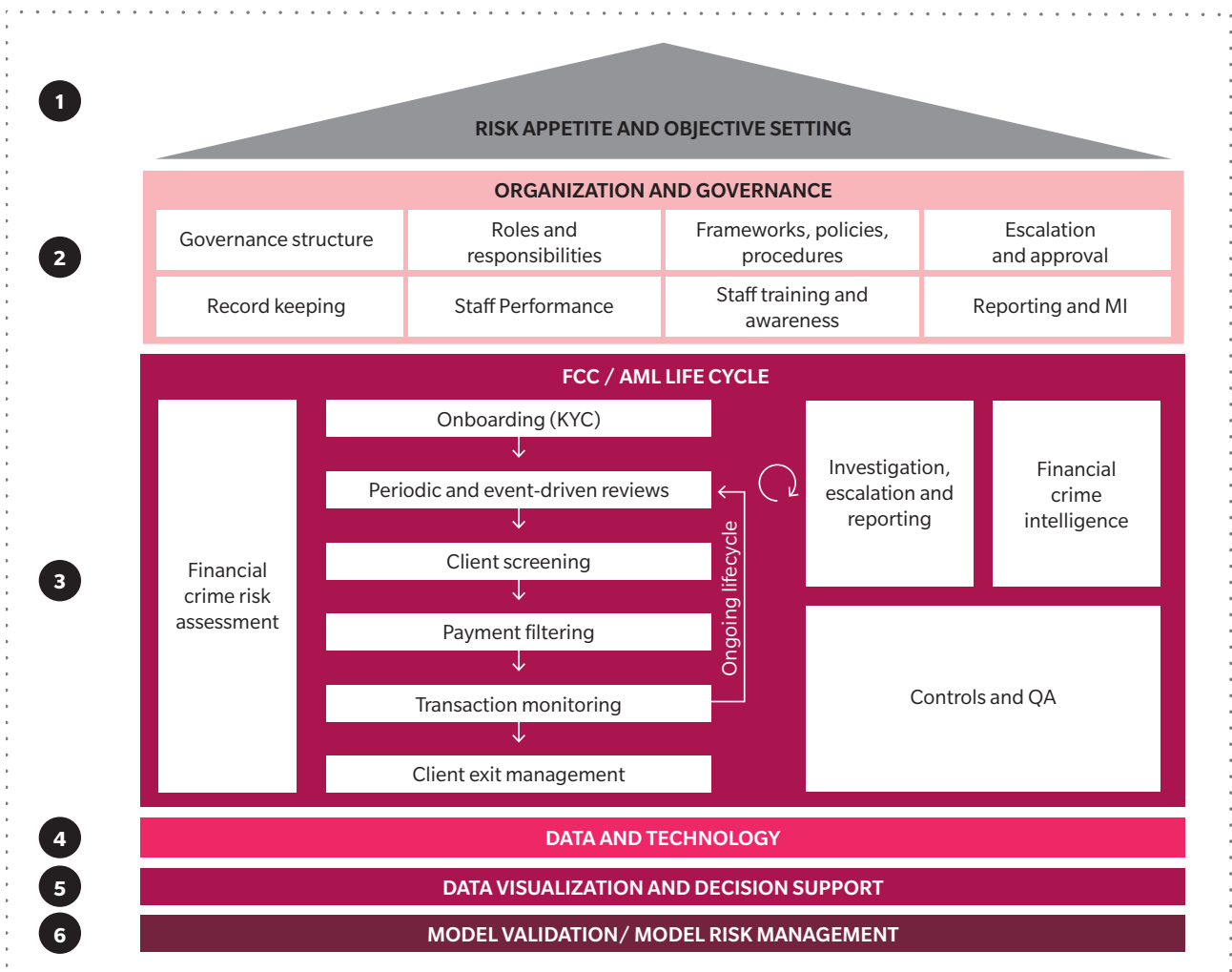
Investigations and case management/ workflow is an area in which there is often underinvestment. Cases are addressed with limited prioritization, which results in the same resource allocation to case files regardless of associated risk. Additionally, while some efficiency and effectiveness metrics may be used for monitoring core processes, few financial institutions are regularly leveraging the results from previous cases to upgrade their alert generation rules or adjust their case handling practices. Next-generation solutions will automate data collection and processing so far as possible, leverage advanced algorithms to pre-assemble case files prior to investigator review, and possess a much more direct and real-time feedback loop to improve performance.

The FCC/AML lifecycle itself should become much more integrated, such that decisions at each point will be informed by both upstream events and downstream impacts. Additionally, dynamic feedback enables much more rapid optimization on an end-to-end basis, across the various silos that often exist today.

4. DATA AND TECHNOLOGY:

At the foundation are the data and systems capabilities which support all analyses and processes. Unfortunately, data is rarely integrated across multiple sources in the bank. This negatively impacts the ability to detect events that are made up of multiple activities, which collectively are suspicious. Additionally, data is often of poor quality in terms of accuracy and completeness, resulting in the generation of excessive false positives. There may be over-reliance on vendor solutions, which may not integrate well to form a robust and flexible systems

architecture. In order to deploy next-generation solutions, institutions will need to put in place a much more expansive and flexible data model and move to a modular solution to seamlessly deploy best-in-class in-house and third-party applications. Updated and improved data and systems infrastructure will also help in meeting more onerous regulatory requirements on end-to-end data integrity and systems robustness, such as NYS DFS 504[1].

5. DATA VISUALIZATION AND DECISION SUPPORT:

Management information used today to monitor activity typically does not support executive- and board-level monitoring of risks and performance in a way that is both holistic and digestible. Institutions could do more to communicate activity, key risks, and performance to management in a more effective manner. Next-generation solutions will include flexible dashboards that provide an up-to-date view of risk, efficiency, and effectiveness to support improved risk management and optimization on an end-to-end basis. This, for example, may better support monitoring and enable a cross-risk type basis (such as across gifts & entertainment, trade cancellations, and market abuse).

6. MODEL VALIDATION/MODEL RISK MANAGEMENT (MV/MRM):

MV/MRM processes for FCC/AML models in the United States are built off the OCC 2011-12 and SR 11-7 regulatory standards, which were largely produced for capital and stress testing and not FCC/AML models. Many institutions have struggled to make MV/MRM work for FCC/AML models due to the complexity of AML risk, as well as the challenges in applying an approach that is

1   See Oliver Wyman Point of View, "Ready Or Not?: Navigating The DFS 504 Rule", www.oliverwyman.com/our-expertise/insights/2018/jan/navigating-the-dfs-504-rule.html

not sufficiently flexible. In order to support next-generation solutions, a robust MV/ MRM framework and processes tailored to the specifics of FCC/AML risk and capable of supporting a broad range in sophistication of modelling techniques, will be required. Such a framework is important for supporting both unsophisticated and sophisticated models.

CHALLENGES TO OVERCOME AND APPROACHES TO DO SO

We see significant challenges to be overcome in four main areas:

1. Data and systems
2. Regulation and urgent remediation needs
3. Accommodating new techniques to improve model accuracy and consistency
4. Bringing along legacy teams to drive transformation through the organization

Whilst not easy we do believe that with the right preparation and approach these challenges can be overcome.

The reference table (See Exhibit 5) provides an overview of these key challenges, and approaches to manage each.

MOVING FORWARD

Transformation of the FCC/AML function will offer significant benefits and many banks are starting to take the right steps. It is important to define the future state and the key steps required, including the new more advanced models and digital tools that will enable improvements in performance and the evolution of the various functions and mandates that will render change achievable and sustainable.

Banks should not wait for perfect starting conditions before beginning; it is possible and arguably necessary to take significant steps even as the critical assets and skillsets that will enable the change are being put in place. Management should prioritize and select initiatives that are meaningful and will produce material results, but not risk stepping too far such that the internal organization cannot keep up or regulatory acceptance comes into question. That said, this is an opportunity that banks should grasp: to drive improved efficiency, improved effectiveness, more comprehensive regulatory response, and more robust management of FCC/AML risks.

Exhibit 5: Overview of key challenges and solutions to overcome

CHALLENGE	DESCRIPTION	SOLUTION TO OVERCOME
Data and systems	Banks will need to capture and manage information from a much broader and richer set of data sources. They will need to deal with multiple fragmented legacy systems and move towards a "single source of truth". While current industry solutions rely on multiple levels of quality assurance to ensure data integrity, next-generation solutions will have to be built off a robust data foundation. Recent data privacy initiatives (such as GDPR) that often diametrically compete with FCC/AML objectives only add to this challenge	Data and system management can involve a diverse set of technology, sources, and stakeholders. There is no "silver bullet" for data updates, and investing to centralize data can often be a significant undertaking. However, creating a centralized source of information and forcing all new solutions to reflect the same "single source of truth" will strengthen solutions that rely on the data, and ensure that everyone in the organization speaks the same language. Facilitating communication by creating detailed data dictionaries and incorporating subject-matter expertise from the business will help the process.
Regulation and urgent remediation needs	Banks in the United States and globally have been under huge regulatory scrutiny, with many receiving enforcement actions and substantial fines. Unfortunately, this has made some banks reluctant to innovate in case they fall outside the "norm" of "accepted practice" or inadvertently expose weaknesses in the system. There are signs that this impasse may at least be beginning to thaw in some jurisdictions; for example, regulators in the United States have indicated that they are open to more efficient and effective approaches	Urgent remediation needs will always be the top priority; however, next-generation capabilities can help increase an organization's resiliency to change over the medium to long term. Providing supervisors with regular updates helps to set expectations and provides an avenue to gather and incorporate feedback. Some banks have found that momentum toward a stronger FCC/AML framework is their most valuable asset to continue to meet and stay ahead of regulatory expectations.
Accommodating new techniques to improve model accuracy and consistency	Modelling in the FCC/AML world is challenging, and a very careful balance is necessary to ensure the right mix of statistical rigor and FCC/AML risk management expertise and ensure that outcomes are robust. The latest advances in ML and AI may in time open up new frontiers. However, careful thought is required not only on where, when, and how to apply these techniques, but how to monitor performance and validate results.	New techniques should be carefully tested before deployment, with significant consideration of how to incorporate risk management expertise. This could include testing synthetic data, or conducting parallel runs of new modeling approaches. New approaches should also be deployed selectively. For many models, there will be a grey zone that represents uncertain outcomes, and other areas where model output is substantially more certain. Models should be deployed given consideration of an institution's risk tolerance.
Bringing along legacy teams to drive transformation through the organization	There is a need to accommodate teams that may come from very different backgrounds and have very different skillsets, but that are in fact all critical to success. Analytics teams need to understand the specificities of FCC/AML risk. FCC/AML risk managers and investigators need to understand the potential of advanced analytics. Legacy IT departments need to be up-skilled to latest tools and agile working methods. MV/MRM needs to be able to accommodate a range of FCC/AML model types and complexities. If stakeholders are not brought along, the transformation will not be successful or sustainable.	Driving transformation through the organization requires a careful stakeholder engagement plan that includes solicitation of feedback as initiatives are developed and deployed. Involving all relevant stakeholders throughout the process will ensure that solutions are fully owned by the business once deployed, not only those who spearheaded development. Similarly, up-skilling a full organization will take time and require a thoughtful combination of training and targeted hiring. The best way to up-skill is to involve the whole organization in the transformation from day one.

3. By way of example, Joseph Otting Head of OCC stated, "We need to reform the BSA/AML to be more efficient while improving the ability of the federal banking system and law enforcement to safeguard the nation's financial system from criminals and terrorists", Testimony before the Committee on Financial Services United states House of Representatives, June 13, 2018

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS	EMEA	ASIA PACIFIC
+1 212 541 8100	+44 20 7333 8333	+65 6510 9700

AUTHORS
Adrian Murphy
Alexander Peitsch
Allen Meyer
Austin Hong
Jayant Raman

CONTRIBUTORS
Alan Morley
Aron Cohen
Chris DeBrusk
Dov Haselkorn
Graeme Jeffery
Stefano Boezio

www.oliverwyman.com

OLIVER WYMAN