FISER CONSULTING
FINANCIAL SERVICES

AML / CTF in the Customer Domain

APRIL 2017

Introduction

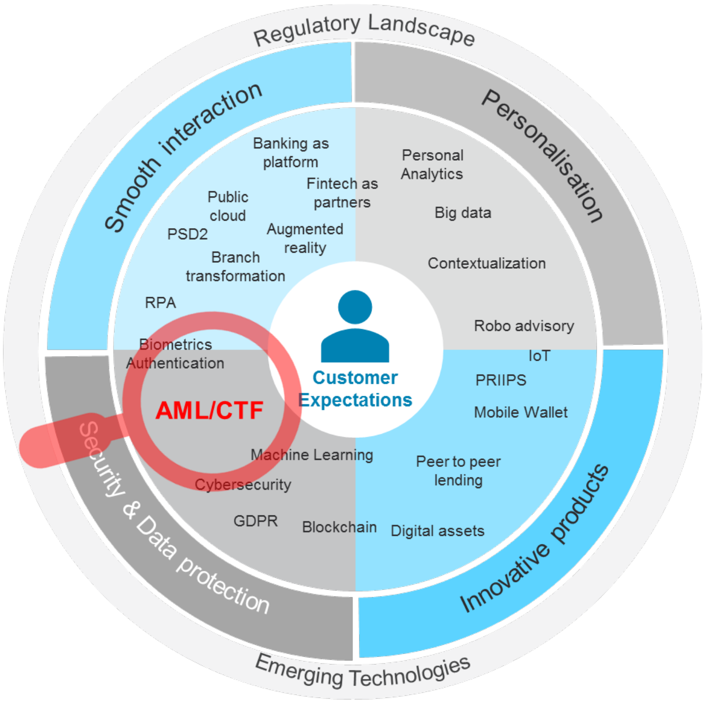
Over the last few years, the introduction of new regulations and the proliferation of emerging technologies have changed customers' expectation of banking products and services. These changes in expectations have had a great impact on the operating model of financial institutions and the way they offer their services and products. Especially in the Customer Domain of these financial services institutions, the consequences of these increased client expectations are felt and institutions need to do all in their power to keep up with the accelerated pace of change to ensure that one the one hand they remain compliant to new and extended regulations while at the same time are able to live up to the increased expectations of its customers.

This paper tries to outline how the customer domain is and continue to be impacted by either new regulations or innovative technology developments in the coming years and more specifically on the developments in the area of Anti-Money laundering and Counter Terrorism Financing (AML / CTF). Firstly, this paper will take a look at the four major categories that integrate the Customer Domain, being either a key regulatory or technologies change that will impact the customer in their daily operations. Secondly, it will show the perspective that FiSer Consulting has on the major action lines for an effective compliance and implementation of the AML / CTF regulations. The main objective of this paper is to be used as a reference to develop a solid strategy that ensures the safeguard of any financial institution.

1. Customer Domain

Several trends compose this evolving customer domain regarding the Financial Services industry. These trends can be classified in 4 major paths: The need for a quicker, easier and more smooth interaction with financial services firms, an increasing demand for innovative products, more personalisation and customisation in client experience, and an enhancement in data protection and transparency.

Figure 1. FiSer Consulting Customer Domain



1.1. Smooth Interaction

Customers are now, more than ever, demanding a more convenient, easy-to-use and quick interaction. One of the main challenges these upcoming years will be to eliminate any friction that still exists in the customer journey and therefore making it as smooth as possible. Several emerging technologies will be able to help in this process. For instance, the use of Robotics Process Automation (RPA) will be key to make processes more efficient and cost-effective. Additionally, the new developments regarding biometric authentication will also add to this enhance customer experience with an easier interaction and improved security.

There is a shift in the banking business model, with banks now acting as a platform for fintech firms. This trend is both regulatory and technology driven, especially enforced by PSD2 and Open banking. This way, financial institutions now must see fintech firms as partners rather than as competitors and create alliances with them to gain a competitive advantage.

Finally, bank branches are not irrelevant, in fact customers still state branch proximity as one of the key factors when choosing a bank, but they must be efficient and invest in new technologies, such as augmented reality, to enhance customer experience.

1.2. Personalisation

Personal analytics, Artificial Intelligence (AI), Big data and contextualization brokering enabled financial institutions to accelerate their digital transformation and provide a more targeted and customised service to each of their clients. Clients are demanding individual solutions and tailored advice from their primary financial institution. Personalisation across the customer journey will be a key differentiation.

The amount of data generated by all the interactions between customers and their financial institutions has increased exponentially. And financial institutions have a real challenge to use this data to adapt the experience of each of their customer when they interact with the different channels of the financial institution to increase loyalty and retention.

1.3. Innovative Products

At the same time, technology has enabled the development of innovative products, which fintech have already started to expand. Digital wallets and digital assets are just a few of the products that the Financial Services industry must provide to their clients in a cost-effective manner. The Internet of Things (IoT) is here to stay and financial institutions have several opportunities to support it with their payments and insurance capabilities. Similarly, the banking industry is heavily investing in blockchain and producing several use cases. On the other hand, the regulatory environment will also affect how products and services are provided, enhancing their transparency and comparability through the

1.4. Security & Data Protection

The increase in data volume and share of information among several parties has created a real concern regarding data protection and security. In addition, the increased connectivity and digitalisation have intensified cybercrime frequency and its impact. Customers will only engage with financial institutions in who they can trust and that take advantage of current technology to minimise risk.

In the past few years, enforcement possibilities of data protection regulators were limited. With KYC, AML and GDPR, this will fundamentally change. Organisations will have to redesign their core business activities to include data protection considerations.

2. Our perspective on AML

2.1. Introduction to AML

Back in August 2011, HSBC suffered from having business relations with Mexican “Cartels”. The sustainability of the whole of HSBC was jeopardised and immediately the rest of the Financial Institutions started to invest in programs to implement controls and technologies to prevent such incidents occurring in their organisation. Six years later, and after a great scrutiny by global and local regulators, financial institutions have not cleared the trial. In February 2017, Rabobank was charged with involvement in misconducts committed with drug cartels. This follows a US investigation about the Rabobank N.A., subsidiary of Rabobank into money laundering in a now closed branch in Mexico.

AML / CTF is a direct threat to the long-term sustainability of any business. In the eyes of the regulators, AML / CTF is critical, because it compromises the reputation and image of the institution. Regulators have shown a little patience with Financial Institutions that lack the internal controls and that have engaged in business relationships with clients that are involved in criminal activities.

However, as any regulatory framework, complying with AML / CTF is a challenge for any Institution. Their major trials arise for the complexity to analyse great amount of information and prevent in a timely matter that unwanted clients use the Institution to fund their criminal activities. In order to develop a sustainable and long term strategy for the implementation, compliance and high performance in the AML / CTF environment, FiSer Consulting has identified five lines of development that will help any Institution reaching its goals.

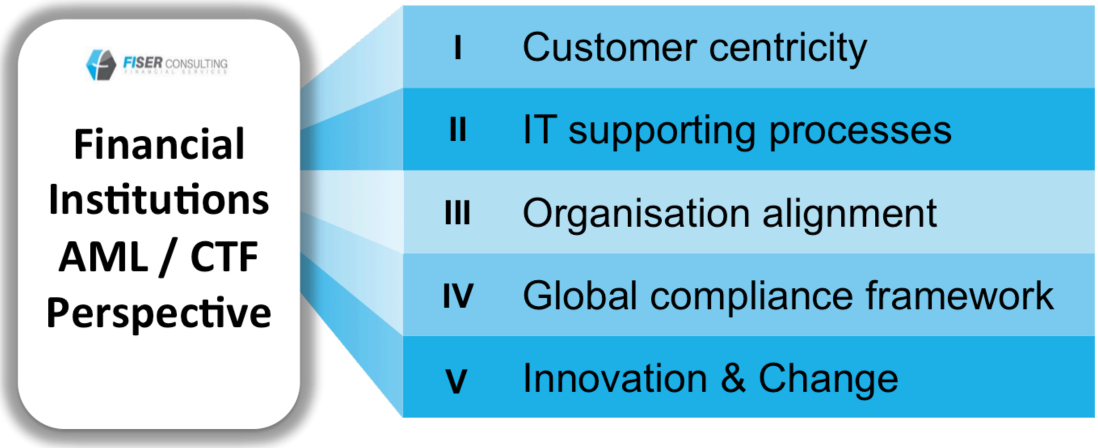

FISER CONSULTING
Financial Institutions AML / CTF Perspective
I Customer centricity
II IT supporting processes
III Organisation alignment
IV Global compliance framework
V Innovation & Change

Figure 2. FiSer Consulting perspective AML / CTF

2.2. Customer Centricity

The main strategic goal is to build a "One-Risk" view per client, that goes across products, services, and units. This perspective has to contain enough information to assess and most important to fully understand the clients' business activities, transactions, and acquaintances. Having this information updated and fully available will help the risk units to determine an appropriate Risk Level that later will be complemented with other Risk metrics to achieve a unified client scoring (retail) and rating (wholesale).

2.3. IT Supporting Processes

The process for the correct AML/CTF operation occurs in four principal stages. Firstly, at the client onboarding, the company has to be fully capable of knowing the intentions and purpose of the client, this moment is called Know your Customer (KYC). Secondly, the financial institution has to gather, safeguard and constantly update important documents and integrate a full client record. Thirdly, an customer based monitoring system (AML) has to be in place to review that each of the transactions operated corresponds to the client's profile. Lastly, all the suspicious transactions that represent a real threat to the institution are subject to a second review.

Specifically, for the customer based monitoring, the risk analyst does an extensive due diligence on the client and their business relations (major clients, stockholders, suppliers). The customer based monitoring methodology is in continuous evolution. Financial institutions are creating strategic alliances with each other to share information and thus, supported by data mining systems, it is more likely to detect suspicious behaviours and report them in a more effective and timely manner to the correspondent authorities. Moreover, the suspicious transactions that represent a real threat to the institution are subject to a more detailed examination. In this "second" examination, the risk analyst can decide to cancel the account or dismiss the client if sufficient evidence was gathered. This moment is called "Case management".

These processes would require an IT tool that not only supports and assist the Risk Analyst in their due diligence but also consolidates the information and presents it across business/products view. There are several solutions in the market (SAS, Norkom, Oracle, to name a few) that follow this methodology. However, the challenge that most institutions face is to build an accurate "one" view report per client. Figure 2, shows the evolution of these processes and explains some relevant activities that happen in each stage. IT infrastructure supports the risk analyst functions.

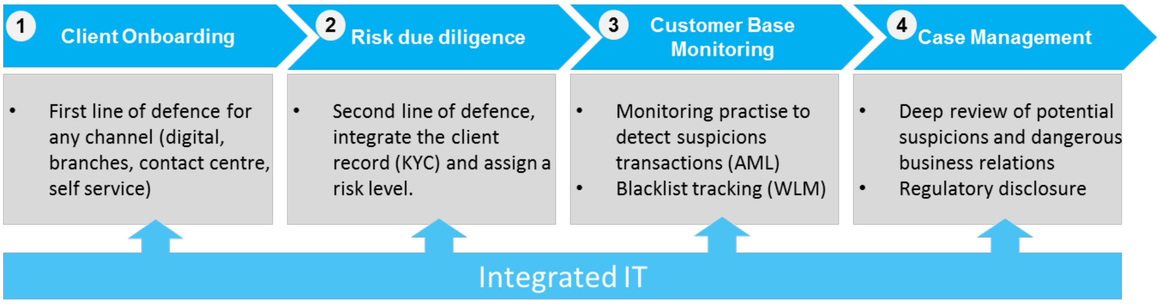

1 Client Onboarding
2 Risk due diligence
3 Customer Base Monitoring
4 Case Management
• First line of defence for any channel (digital, branches, contact centre, self service)
• Second line of defence, integrate the client record (KYC) and assign a risk level.
• Monitoring practise to detect suspicions transactions (AML)
• Blacklist tracking (WLM)
• Deep review of potential suspicions and dangerous business relations
• Regulatory disclosure
Integrated IT

Figure 3. Process and IT Integration AML/CTF

2.4. Organisation Alignment

Depending on the maturity of an institution and the degree of specialisation of the staff, the organisational structure and functions distribution can differ. Figure 3 shows the four levels of how a financial institution can control and manage its AML/CTF processes. The desired level is called "Autonomous Staff". At this level, each risk analyst will be responsible for the dismissal or trace of the suspicious activities detected, from their detection to their closure. At this level, the organisation relies completely on the capacity and judgement of each of the risk analysts whose scope would reach the four stages of the AML/CTF. To reach this level, accuracy of data, reliability of IT systems and a flat organisation are a pre-requisite.

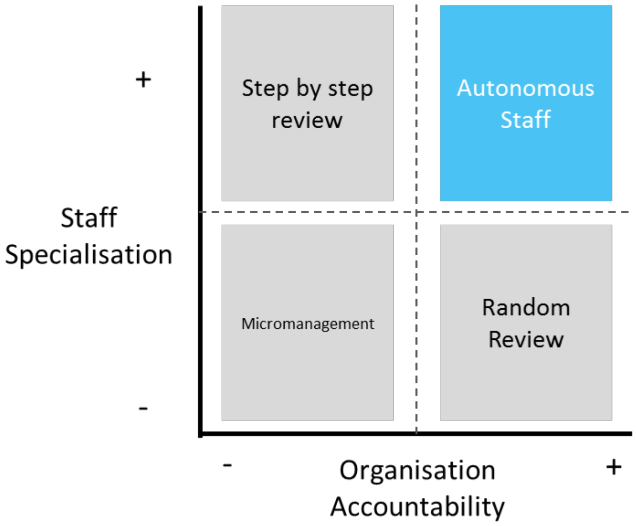


Figure 4. Organisation maturity matrix

The second phase of development is the "Random Review" level. At this level, even when the staff have not acquired full specialisation, they are still responsible for the result of its work. For this level, the financial institution would have a "Quality Assurance" department that would review from time to time a random sample of cases and would conduct a secondary analysis, ensuring the correct result.

The "Step by step review" and the "Micromanagement" belongs to companies that are in early stages of development and still don't fully rely on the work conducted by the risk analysts. Additionally, these institutions do not have informational systems that provide solid and concise data. The institutions that stand at these two levels need to unify the analysis and risk criteria among the team, to ensure data quality in their systems, and to invest in the development of internal talent.

2.5. Global Compliance

Financial institutions that have operations in multiple regions should built a global compliance framework. This framework should take into account the one proposed by different authorities, such as ECB, BIS, IMF and BSA. Additionally, best practices and publications provided by associations such as ACAMS and ICA should be considered.

The integration of a global framework will allow the organisation not only to build a solid local policy but also to gain sufficiently flexibility to comply with policies in other jurisdictions, where the company has businesses. This practice will allow to share global consistent information first inside the group and to regulators and other financial institutions. Finally, this unified perspective will help the institution to fully understand the key risks elements per geography.

2.6. Innovation & Change

Financial institutions need take this opportunity to prepare for the adoption of emerging technologies, especially RPA and Blockchain. The booming technology trends will change for good the AML / CTF function from an operating/compliance to an analysis/decision-making mode. As mention previously, it is the role not only of the Risk & Compliance areas but also of the Business Units to prepare for the implementation and operation of the following technologies:

- **Blockchain:** This technology might offer an enormous range of opportunities for the financial industry, creating a completely different economy, threatening the "middle man", in this case, the financial institutions itself. Until now, banks and insurance companies had been smart enough to embrace change and explore alternatives to profit from this technology. In the AML / CTF processes and controls, the implementation of Blockchain would transform the way to protect the institution. Blockchain would entail:
    - Full Transparency: All operations of a client will be recorded in a general ledger, with this data structure in place, the institution can trace the origin – destiny of any resource and determine if a client is trustworthy to do business with.

    - Global Cooperation: Under the general ledger, all the Financial Institutions, Governments and private entities will be connected. This stage of entire connectivity will allow that institutions will fully know their clients.

- **Robotic Process Automatization "RPA":** Financial institutions need to prepare to implement this technology by firstly identifying and separating the strategic functions from the mechanical ones. As it can be predicted, the staff, that is involved in pure mechanical activities, is at risk of being replaced. However, if the same staff takes accountability and leadership for strategic functions, RPA has the potential to become a great ally. Finally, the institution needs to have consistent historical data to fully exploit the capabilities of the RPA tools.

Next steps

For further information on AML / CTF and where FiSer Consulting can assist you, please contact:

FiSer Consulting | Paul Nielsen

This Project Manager has over fifteen years of financial services and management experience across retail banking, investment banking, asset management, accounting, IT and FMCG sectors. Extensive AML and Sarbanes Oxley experience in the UK banking sector as well as having managed high profile projects across different business areas and service offerings.
Contact: p.nielsen@fiser.consulting

FiSer Consulting | Roberto Nieves

Roberto has over 5 year’s experience as management consultant, leading and promoting change for top financial institutions. Roberto’s consulting skills are mostly in change/project management and business strategy. He has participated in relevant Anti-Money Laundering (AML) and Know-Your Customer (KYC) projects in the areas of compliance, operations, processes and organisation.
Contact: r.nieves@fiser.consulting

FiSer Consulting | Constanza Diaz

Constanza has over 2 year’s experience in Management Consulting. She has gained extensive experience working in a wide range of industries such as Financial Services, Retail, Utilities, Pulp & Paper, and Insurance, and different Finance related sectors such as Business Development, Risk Management, Project Evaluation and Strategic Planning.
Contact: c.diaz@fiser.consulting

FISER CONSULTING
FINANCIAL SERVICES

Barbara Strozzilaan 201
1083 HN Amsterdam
The Netherlands

Tel.: +31 20 20678386
www.fiser.consulting