Optimization of KYC Processes – Squaring the Circle?
Background

KYC processes are among the most complex workflows of a bank’s process landscape. For years, one KYC project has followed another to introduce new regulatory requirements, reduce costs and risks, and enhance user experience. In the past, banks took organizational steps to improve KYC processes. However, the potential of such organizational steps has largely been realized. For this reason, most banks are now focusing on digitalization. They are introducing new tools and technologies that – if used appropriately – will be able to reduce risks and costs significantly and enhance user experience substantially. Yet there have been very few successful KYC digitalization initiatives. Where do so many banks go wrong in their attempts to digitalize their KYC processes?

With the revision of the Swiss Anti-Money Laundering Act and Ordinance-FINMA (AML-A and AM-LO-FINMA), this question is becoming even more relevant: Presumably starting in January 2020, banks must regularly update KYC-relevant client data, stronger align KYC standards globally, and more systematically verify beneficial owner information. If implemented manually, these additional requirements will significantly add to the costs and complexity of banks’ KYC.

This whitepaper looks into the question of pitfalls and success factors of KYC digitalization and present potential solution approaches.

Definition of KYC (know your client)

KYC in the narrower sense: Review of the identity of new clients to prevent money laundering in accordance with statutory provisions

KYC in the wider sense (as used in this whitepaper): Collection and review of client information to meet all regularly applicable statutory requirements as part of the client onboarding and monitoring of the relationship

1 At the time of publication, the consultation process of the Federal Council is planned until September 21, 2018
When it comes to the digitalization of KYC processes, successful and less successful banks can be distinguished by their approach. The successful ones have a clear understanding of the challenges they face in KYC and the priority to address these challenges. They have a digitalization strategy and a vision of how KYC processes, the organization, and the architecture should look in the future. They have a realistic roadmap that allows for quick wins. They have a comprehensive and continuous view of KYC processes rather than focusing on individual process steps. They establish the requisite expertise internally so that the future projects can be handled by the current team without the need for external advisors. This may make sense at the beginning to quickly make the first progress. Over the course of the project, however, expertise should be developed internally so that the future organization will be able to take over when the advisors leave the bank.

At less successful banks, the digitalization of KYC processes often degenerates to a simple tool selection exercise. A request for proposals is initiated without a clear sense of the problems that need to be addressed, not to mention the definition of business requirements or a target operating model. Frequently, only parts of the KYC processes are considered, which precludes a comprehensive solution from the outset. There is also often a lack of cross-departmental collaboration. Furthermore, less successful banks often rely heavily on external advisors. This may make sense at the beginning to quickly make the first progress. Over the course of the project, however, expertise should be developed internally so that the future organization will be able to take over when the advisors leave the bank.

1. Holistic digitalization strategy with clear goals
2. Collaborative approach with a front-to-end process view
3. Transformational approach: Digital agenda led from the top with central execution
4. Early internal build-up of know-how and cultural change (client focus, agility, collaboration)
5. Focus on «Change-the-Bank»
6. Agile and collaborative project methodologies (e.g., interdisciplinary teams, early and continuous feedback)

1. Feature selection and me-too approach
2. Organizational silos along functions
3. Tactical execution of one-off, disconnected projects
4. Heavy reliance on external resources with lack of internal buy-in and know-how
5. Focus on «Change-the-Bank»
6. Focus on cost cutting and employee replacement
7. Traditional implementation methodologies (e.g., waterfall development)

When it comes to the digitalization of KYC processes, successful and less successful banks can be distinguished by their approach. The successful ones have a clear understanding of the challenges they face in KYC and the priority to address these challenges. They have a digitalization strategy and a vision of how KYC processes, the organization, and the architecture should look in the future. They have a realistic roadmap that allows for quick wins. They have a comprehensive and continuous view of KYC processes rather than focusing on individual process steps. They establish the requisite expertise internally so that the future organization will be able to take over when the advisors leave the bank.

At less successful banks, the digitalization of KYC processes often degenerates to a simple tool selection exercise. A request for proposals is initiated without a clear sense of the problems that need to be addressed, not to mention the definition of business requirements or a target operating model. Frequently, only parts of the KYC processes are considered, which precludes a comprehensive solution from the outset. There is also often a lack of cross-departmental collaboration. Furthermore, less successful banks often rely heavily on external advisors. This may make sense at the beginning to quickly make the first progress. Over the course of the project, however, expertise should be developed internally so that the future organization will be able to take over when the advisors leave the bank.

1. Holistic digitalization strategy with clear goals
2. Collaborative approach with a front-to-end process view
3. Transformational approach: Digital agenda led from the top with central execution
4. Early internal build-up of know-how and cultural change (client focus, agility, collaboration)
5. Focus on «Change-the-Bank»
6. Agile and collaborative project methodologies (e.g., interdisciplinary teams, early and continuous feedback)

1. Feature selection and me-too approach
2. Organizational silos along functions
3. Tactical execution of one-off, disconnected projects
4. Heavy reliance on external resources with lack of internal buy-in and know-how
5. Focus on «Change-the-Bank»
6. Focus on cost cutting and employee replacement
7. Traditional implementation methodologies (e.g., waterfall development)
2. Developing the Target Operating Model

Once the challenges have been analyzed and pain points prioritized, the target operating model should be developed. In addition to the objectives, the target operating model describes end-to-end processes, the future organization, the data model, the IT architecture, and the ecosystem.

Definition of Goals

Concrete objectives enable clear planning and prioritization, facilitate communication of the KYC digitalization strategy, and permit measurement of success. Therefore, after the analysis of pain points, the KYC digitalization strategy should be developed, including a prioritization of the pain points and answering the question of what shall be achieved with the digitalization of KYC processes. The answer will be different for every institution and is determined inter alia by the business model and size of the bank. In any case, the digitalization strategy should contain short term quick wins and KPIs.

Definition of Target Processes

Automation alone cannot resolve process difficulties that lead to long onboarding times and frequent client interactions. Therefore, the onboarding process should be analyzed holistically regarding which client data is required at what point of the process and what controls should be performed to minimize both the number of interactions and the amount of data collected at any point. The analysis should consider different business segments requiring different processes. Banks with foreign branches will need to answer questions around global minimum standards to harmonize KYC processes and whether certain KYC services should be provided centrally.

**Are onboarding times, client interaction, and switching of channels a topic for your institution?**

**Ask your clients and conduct a Voice-of-the-Customer.**

---

*KYC Risks*

Most banks continue to use manual processes and controls in compliance. With the extension of KYC checklists by FATCA, AML, and MiFID controls, compliance employees now have to conduct between 15 and 30 tests with different controls – including such complex tests as FATCA and AML «reason to know» tests and KYC risk classifications. Not surprisingly, this leads to an error rate of 10-30%, depending on the client segment. Consequently, many banks have extended secondary controls, resulting in increased costs. Due to the manual processes and controls, there is often a lack of client data plausibility checks – especially cross-regulatory checks. KYC, FATCA, AML, and MiFID require the collection of similar data, but the data is not cross-checked regarding consistency. Supervisory authorities have a clear point of view on such inconsistencies: All client data collected by the bank must be considered when assessing the client and inconsistencies are to be rectified.

In general, regulatory scrutiny has increased significantly. Review programs become more and more comprehensive and consider not only adherence to laws but also to internal policies. For banks with foreign branches and subsidiaries, KYC risk assessments are newly performed on a global basis. Therefore, costs have risen sharply in recent years because of new regulatory requirements. For example, the number of employees who review client information and formalities as part of KYC processes has increased by an average of nearly 20% per year (which corresponds to a doubling of costs over a period of ten years). Large institutions have more than 300 employees working in their compliance departments on KYC processes and even smaller banks now employ ten or more people for KYC. Nevertheless, costs are likely to further increase in the next years with the revision of AMLO-FINMA, which requires client data to be regularly updated and beneficial owner information to be verified.

But not only the costs of the current KYC operation have increased. Many banks invest tens of millions every year in implementing new regulatory requirements.

**How effective are your KYC controls, and are global standards a topic for your bank?**

**Test control effectiveness and assess risks systematically and globally.**

**Costs**

KYC costs have risen sharply in recent years because of new regulatory requirements. For example, the number of employees who review client information and formalities as part of KYC processes has increased by an average of nearly 20% per year (which corresponds to a doubling of costs over a period of ten years). Large institutions have more than 300 employees working in their compliance departments on KYC processes and even smaller banks now employ ten or more people for KYC. Nevertheless, costs are likely to further increase in the next years with the revision of AMLO-FINMA, which requires client data to be regularly updated and beneficial owner information to be verified.

But not only the costs of the current KYC operation have increased. Many banks invest tens of millions every year in implementing new regulatory requirements.

**How effective are your KYC processes?**

**Calculate your savings potential and establish a spend-to-save business case.**

---

**Synpulse observation during several projects.**

3 The requirements for a global KYC surveillance system will continue to increase in 2020 with the revision of the Anti-Money Laundering Directive-FINMA (AMLO-FINMA) and the Swiss bank’s code of conduct with regard to the exercise of due diligence (both expected to apply from 2021).

4 Thomson Reuters 2017 Know Your Customer Surveys.

---

**3 Elements of the target operating model.**

For a private bank, the support of the client advisor (e.g., using a tablet solution) is more relevant than allowing clients to do as much as possible on their own (e.g., with end-to-end online self-onboarding). For a retail bank, the strategy will be the other way around in this regard. A large institution will be more likely to automate controls to reduce costs, while a small institution may want to stabilize processes to decrease risks.
Finally, target onboarding processes should be developed in a way that facilitates leverage for managing changes in circumstances and reviews. This helps to avoid inconsistencies in KYC controls and decisions and allows to use the same tools and services for different KYC processes. This aspect becomes even more relevant with the revision of the AMLA and AMLO-FINMA expected to be applicable in 2020 when client data must be regularly updated.

Definition of the Target Organization
The digitalization of KYC processes will have a major impact on the current organization. It will result in the loss of some roles and the introduction of new ones. For new roles, governance, role profiles, and resources must be defined well in advance. For example, when using rule engines, the tasks and responsibilities for defining, coordinating, and deciding on rules should be defined at an early stage. In light of the AMLA and AMLO-FINMA revision, this governance should ideally be defined globally to meet the new requirements of a global KYC control framework. Similarly, a ‘KYC change authority’ should be established taking decisions about future changes to KYC processes.

Definition of the Data Model
KYC processes are all about data collection and analysis—primary KYC data banks need to collect with law and secondary KYC data banks collect, e.g., marketing purposes or a deepening of client relationships. To comply with data protection law, it is important to understand at every point of data collection and analysis, the purposes and legal grounds of data processing.

Another aspect of the data model is the level at which data are collected and processed—e.g., product-level, relationship-level, or person-level. Furthermore, data repositories should be designed as centrally as possible to, e.g., avoid inconsistencies or additional controls, meet minimization requirements under data protection law, and facilitate client data management through different channels including switching during account opening.

Analysis of the Options for Using Technologies
After definition of goals, processes, the organization, and data model, it is time to look at technology. Especially for larger banks, no single solution will meet all requirements. Instead, technologies must be combined sensibly. Here, the target IT architecture and its integration into the current system landscape is critical. The following section sheds some light upon technologies often referred to as ‘digitalization’.

1. Business Process Management (BPM) Software
BPM platforms help to manage the flow of information and tasks along a process chain involving several people. They are well-suited for supporting the collection of client data and performance of manual controls, such as the analysis of PEPs, sanctions, or negative news hits. They ensure that employees adhere to the defined process and can integrate various KYC services such as KYC, FATCA/JAVA, or OFAC controls, background checks, video ID solutions, and client risk classifications. For this reason, they often form the foundation for the digitalization of KYC processes. Most work-flow platforms offer visual process design (‘low code platform’), meaning they do not require technical expertise and can also be implemented by business experts.

Where possible, process steps should be parallelized to reduce onboarding times. With case management, an onboarding case can be processed by several people at the same time (e.g., by the PEP expert and the specialist for reputational risk).

2. Rule Engines (Decision Model and Notation (DMN) Software)
Rule engines permit the bank to separate KYC rules from processes and applications and thus allow to keep KYC processes and core banking systems stable over a longer period, while rules frequently change. Because rule engines provide visual rule design (‘rule tables’), all rules can be seen at a glance including the rules hierarchy and be modified without coding.

Besides, rules and controls can be defined and managed centrally and provided as a global service to various processes and systems in different countries. This reduces change and harmonization efforts and reduces the risk of inconsistent KYC standards. Moreover, using a rule engine ensures that decisions and controls are carried out per defined criteria and not based on employees’ abilities (or daily whims). Furthermore, when controls and checks are largely automated, banks can easily introduce additional controls, avoid manual errors, accelerate KYC processes, and reduce KYC costs.

Most providers allow new rules to be tested and calibrated before they are deployed. This helps to avoid unpleasant surprises. In addition, rule engines typically offer versioning and documentation for audit purposes.

3. Scanning and ID Solutions
In the past, scanning solutions were mainly used for electronic archiving of paper forms. The new scanning solutions can identify and record client data (even in handwriting) and check signatures.

Furthermore, scanning solutions are more and more used for client identification. They can scan clients’ IDs and verify them using facial recognition (i.e., taking a picture and then comparing it with the ID photo.) Also, they can read and check security data and personal and biometric information from the ID chip. By using this three-factor check, clients can be identified quite reliably. Nevertheless, most regulators, including FINMA, still require additional identification by a person (e.g., through a
video chat) or a domestic payment (in future: payment from a FATT-compliant country).

As an alternative to personal identification, some countries already offer the option of using an electronic ID, which involves a one-time identification of the client by a public or private agency. This electronic ID can then be used to open a bank account. In Switzerland as well as on European Union level, there are several initiatives working on the introduction of such an electronic ID.

4. Blockchain

Several private and public-private initiatives have been launched in recent months to test the use of blockchain technology for KYC purposes. These approaches are based on the KYC utility idea under which a client is identified and documented only once by a participating financial institution or the central utility for various regulatory purposes. The other participating institutions can then access this information provided on a shared platform (managed by the utility) when opening new relationships, rather than having to re-collect and verify the data again. In the blockchain solution, the utility is replaced by the so-called “distributed ledger” – offering the advantages of lower costs, a high level of security, the immediate availability of new data for all banks, and an audit trail, as the ledger contains all historical data. Some banks are also testing blockchain technology internally to simplify KYC processes globally.

Due to the technical complexity and open data protection and regulatory questions, it is not yet possible to predict whether and when blockchain will be used for KYC purposes on a wider scale. From a data protection point of view, the risk regarding a correct client identification for KYC, FATCA, MIFID, etc. remains with the bank, despite delegating some KYC steps to (unknown) third parties in the blockchain.

5. Robotic Process Automation (RPA)

RPA is a technology that allows the automation of clearly defined processes based on existing applications. Because RPA does not require a technical integration, but instead builds on the user interface of existing applications, it provides a quick-to-deploy, non-invasive option for automation. RPA is a technology that automates well-defined processes based on existing applications. Not surprisingly, most banks are already using RPA or are at least considering feasibility studies. Because RPA builds on existing applications, however, this technology generally does not achieve the level of performance of a fully integrated rule engine or BPM software. For this reason, RPA is particularly suitable for supporting ad-hoc KYC reviews or for a slight integration of a rule engine if a bank is reluctant to build all interfaces in an early adoption phase.

6. Analytics und Screening Tools

Analytical and screening tools are algorithmic processes that search through (structured) data for certain patterns or information and combine, prepare, and provide such information in aggregated form. As they are used, for example, for negativ news, PEP, and sanction screening. Banks traditionally use standard solutions from established business information providers, which usually only allow for predefined and quite simple searches. To allow a margin of error for client segments with increased risks, it is recommendable to use the raw data from such providers, but alternative search functions with more flexible search algorithms. Another weakness of traditional search solutions is their limited ability of recognizing relationships between persons. Newer screening tools use the world-wide web as a data source and use artificial intelligence to recognize relationships. In addition to KYC, analytics and screening solutions are also used for transaction monitoring (KYT). With the revision of the AMLA and the ML-D-FINMA, transaction monitoring will become even more important, as KYC data needs to be updated regularly which is partially available through transaction information, and KYT results in turn are to be considered for the KYC risk classification. While the use of such technologies for KYC purposes appears to be attractive, the effort should not be underestimated: Models need to be calibrated and the quality of the methodology evidenced by control validations. Further, data protection requirements need to be considered.

7. Artificial Intelligence (AI)

AI can be used in a couple of KYC processes, including background screening to assess large volumes of unstructured data and to identify connections between the client and third parties for which PEP, negative news, or sanction information is available. In addition, AI can be used for KYC risk classification and transaction monitoring.

Because AI is based on correlations and not on causality (i.e., pre-defined rules), the primary challenge is the validation of the quality of decisions taken by AI and its explanation to the supervisory authorities. AI is usually not for situations with only a few data points and, even in cases with a high data volume, banks are still reluctant to use AI and tend to apply it only in KYC support processes. For example, in the form of hybrid chatbots that support the client or client advisor if they have questions or for completing and testing traditional KYC procedures.

8. Apps and Multi-Channel Integration

Many banks now offer their clients the option of opening an account themselves online or via their mobile device and changing client data via these channels. Thus, together with the client advisor, the branch, and the hotline, clients can use up to five channels to interact with the bank concerning KYC data. While an app or online solution can be developed quickly, the subsequent integration in the bank’s processes is much more difficult. On the one hand, the same controls must be applied across all channels. On the other hand, channels must also be mutually permeable, i.e., offer the possibility to switch between channels. If the client drops out of the online account-opening process and instead calls the hotline, the call center employee must be able to authenticate the client and access the data that has already been entered. This requires central data storage across all channels and a secure authentication mechanism. Omichannel platforms facilitate the management of different channels.

Identification of Partners

Transparency on solutions and providers in the market is key to take the right “make-or-buy” decisions, select the right partners, and build up an ecosytem which is sustainable in the long-run. Other prerequisites for a successful partner selection include the definition of precise requirements, a business case, a proof-of-concept with clearly defined targets and KPIs, an appropriate sourcing model, and controls agreed in the beginning of the collaboration.

3. Project Approach

Once the target vision has been defined, a realistic roadmap for implementation should be developed – including some quick wins.

With respect to the project organization, collaboration across departments in interdisciplinary teams is essential. Otherwise, the front office will digitalize its parts of the KYC process independently of compliance, compliance independently of IT, and IT will carry out its own digitalization project. This will result in a patchwork of tools and partial automation, and none of the departments will achieve their objectives. To foster collaboration and speed up implementation, it may make sense to use elements of agile project methods. At the same time, it is essential to ensure an audit-proof project approach and implementation in accordance with regulatory requirements through all project phases.

To reduce double work and pushback, it should be clarified right at the start of the project, how existing initiatives that impact KYC processes will be handled. As KYC projects impact all areas in the bank, communication about the project should be transparent, comprehensive, and continuous. Stakeholders, such as client advisors and compliance employees should be involved early on. This will increase the acceptance of new KYC solutions.

Add to this the active support of senior management, and nothing stands in the way towards the digitalization of KYC processes.
Conclusion

KYC processes are among the most complex processes at banks. Costs and risks have risen significantly in recent years driven by the numerous new regulatory requirements. For clients – especially in private banking – opening a banking relationship has become a tedious experience. Digitalization offers several solutions to address these challenges. However, not all banks have been successful in implementing these solutions. The success factors include:

1) A thorough analysis and prioritization of pain points
2) A KYC digitalization strategy underpinned with a business case and KPIs
3) A target vision defining the future organization, an end-to-end process view, an appropriate data model, the IT architecture, and a sustainable ecosystem
4) A roadmap that is realistic and allows for quick wins
5) A project organization that is based on interdisciplinary teams and close collaboration across different departments
6) An audit-proof project approach and disciplined implementation

Based on our compliance and technology expertise, consulting experience, and project management know-how, we can help you to successfully follow the path towards KYC digitalization and effectively apply new technologies.
Appendix

Author

Tina Freund
Co-Lead Regulatory & Compliance
tina.freund@synpulse.com

Co-Authors

Matthias Eberhard
Advisory and Training Solutions
matthias.eberhard@synpulse.com

Heiko Fischer
Topic Expert Customer Intelligence & Big Data Analytics
heiko.fischer@synpulse.com

Adrian Hartmann
Head Client Lifecycle Management
adrian.hartmann@synpulse.com

Andrea Lorenzo Solèr
Workflow Platforms
andrealorenzo.soler@synpulse.com

Eric Stehli
Head Regulatory & Compliance
eric.stehli@synpulse.com

David Steiger
Robotic Process Automation
david.steiger@synpulse.com

Andrea Weber
Regulatory & Compliance
andrea.weber@synpulse.com
About Synpulse

Synpulse is a multinational management consultancy and valued partner of renowned financial service providers around the globe. Our locations at the financial industry hubs, our wide range of services and our extensive industry expertise are the basis for our outstanding and bespoke results. We support our clients in the development, the realization and the implementation of their corporate strategies. Together we meet and anticipate challenges in the organization, the processes and the systems.

Industry Focus
Our particular expertise is dedicated to the industry-specific challenges of financial service providers. Leading private and retail banks, direct insurers, health insurers and reinsurers trust us.

Expertise
Synpulse offers its clients comprehensive performance during all phases of a project. Our consultants support our clients in the technical, organizational and technological realization of projects.
Switzerland
Zurich (Headquarters) | Geneva

Germany
Dusseldorf | Frankfurt | Ulm

United Kingdom
London

Singapore
Singapore

Hongkong
Hongkong

USA
New York

Austria
Vienna

Slovakia
Bratislava

info@synpulse.com
synpulse.com