Compliance 2025– Preparing the Compliance function for the digital age

INTRODUCTION

Accelerated by the COVID-19 pandemic the financial sector is currently going through a substantial digital transformation of business and operating models, mainly to cater for changed customer expectations and behavior and optimize the efficiency of banking operations.

Digitization disrupts the way banks do business. Physical customer interaction and the manual orchestration of product and service requests move to the background, while key processes are being automated, from the customer interface to workflow solutions, straight through processing of repetitive tasks, and the automated integration of internal and external data. The digital age has in store several promises which make banking more effective and more efficient, and compliance functions are likely to profit from them. However, compliance functions need to get prepared for the changes that lay ahead and fully embrace the potential disruption that comes with it, particularly around two main trends. First, the development of products and client solutions will happen faster, more dynamically, and more frequently. Compliance functions need to adapt to these new dynamics, turn proactively towards the business, understand agile ways of working, and anticipate the opportunities to get involved early in the process. Second, data is the new gold. Banking business is increasingly digital, and the work of compliance functions will be more data driven and less paper based, manual, and reactive. Compliance functions which seize the opportunity will emerge stronger, and those who do not will fall back. The digital age will revolutionize the way compliance functions work and must be tackled with determination and a dynamic mindset open to change.

This paper discusses six key factors which we believe are essential in successfully transitioning compliance functions to the digital age. They are:

1. What supervisors expect from compliance in the digital age– compliance functions must understand what will change, and where
2. Digitization impacts bank's risk exposures– a sophisticated risk appetite framework is required to stay clear of dangerous territory
3. Automation and opportunities for artificial intelligence (AI)– compliance functions should make use of new technologies to optimize their operations

4. Along with digitization comes "agile" – compliance functions need to prepare for new ways of flexible and dynamic working

5. Skill profiles of compliance officers– technology, data, and AI will play an even bigger role in compliance work

6. Cooperation across financial institution– an option to make compliance operations more sustainable in the digital age (?)

1 The digital age: Supervisory expectations the Compliance function must anticipate

The ongoing digital transformation of the financial sector has resulted in an increasing supervisory focus on digital business and operating models.[1] This impacts several bank stakeholders including the Compliance function which needs to anticipate regulatory expectations in three key areas described below. Above all, supervisors need to trust that Compliance functions can deliver effective risk oversight in a digital setting.

1.1 TECHNOLOGY, SYSTEMS, AND DATA LANDSCAPE

Depending on business model, IT landscape, client universe, and other factors digitizing key banking processes such as sales, onboarding, customer due diligence, and settlement often results in multi-layered, inter-connected operating models. These often include client self-service portals, case management and workflow tools, data layers integrating e.g., core banking systems and credit decisioning applications, third party data services and hardware components. Each of these layers often cover different components to cater for diversified product, transaction, and client needs. The compliance function must raise (regulatory) concerns if digital operating models do not meet regulatory requirements e.g., on the handling of customer data, record keeping, or control effectiveness. Compliance should also monitor that changes to the regulatory environment are effectively embedded in digital operating models, and measures are implemented to protect against e.g., cyber and fraud risk.

1.2 DIGITAL PRODUCT AND SERVICE PORTFOLIOS

Digital transformations of bank's circle heavily around leaving traditional, physical use of services and products towards portfolios that area available at customer's fingertips, whenever they need them. Physical customer interaction is replaced by digital client channels, live chats, or even chat bots. In a digital environment mandatory checkpoints for regulatory conformity such as a new product process or product specific 1st line of defence and/ or Compliance approvals must remain fully embedded. To ensure full conformity, the compliance function should monitor regulatory implications resulting from the switch to digital product portfolios, raise alerts when required, identify action areas, and (where required) escalate to senior management.

1.3 ARTIFICIAL INTELLIGENCE

Digitization multiplies the volume of data available to financial institutions and opens increasing opportunities to deploy artificial intelligence ("AI"). AI in turn is increasingly subject to regulatory requirements. Even though the maturity of AI regulation is uneven across jurisdictions the key expectations of regulators towards financial institution's deployment of artificial intelligence can be generalized along three core themes: Governance (incl. full senior management accountability for AI applications), design and development (incl. ethics and fairness, data quality, and technical documentation), and ongoing maintenance (human oversight, periodic reviews, and risk management).[2]

During or towards the end of the design process targeted AI applications need to be checked against regulatory requirements and potential shortfalls need to be addressed. The Compliance function should be required to perform the review or validate the main results.

2 Compliance-by-design: Steering the business with a contemporary risk appetite framework

Digitization impacts the risk exposure of financial institutions. Some risk types become more relevant (e.g., cyber, IT availability, digital ethics) while others may stay but less in the spotlight (e.g., physical workplace safety). COVID-19 accelerated the exposure of financial institutions to heightened risk in some areas, e.g., limited oversight on systems and tools used by employees for daily work, blurred boundaries between private and professional life decreasing employees' awareness for potential Compliance issues (e.g., printing sensitive material at home). The risk-based approach, propagated by all major financial regulators and standard across leading financial institutions, is becoming ever more relevant in the digital age. Focusing compliance oversight on areas with increased compliance risk and quickly adapting to changes in the risk profile will be increasingly required in

[1] See e.g., ECB's SSM and BaFin's supervisory priorities for 2021 with a strong focus on assessing bank's progress in response to the accelerated digital transformation.

[2] For more details on the regulatory approach to AI in the financial sector please refer to the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act); High-level principles on artificial intelligence, Hong Kong Monetary Authority, November 2019; and Principles to promote fairness, ethics, accountability and transparency in the use of artificial intelligence and data analytics in Singapore's financial sector, MAS, November 2018.

institutions with a strong digital footprint. More dynamic client offerings, higher frequencies of product development, and overall less predictability in medium or long term strategic planning will challenge the way compliance functions have traditionally operated.

Hence for banks, defining their own risk appetite and taking measures to steer the business on a risk-based approach is ever more essential. A risk appetite framework ("RAF") represents the overall approach through which risk appetite is established, communicated, and monitored. It should include qualitative risk appetite statements, key risk indicators, and quantitative risk thresholds. If meaningful quantitative risk thresholds and limits cannot be defined for certain non-financial risks, the RAF instead needs to outline dedicated qualitative risk appetite statements for these risk types.

2.1 QUALITATIVE RISK APPETITE STATEMENTS

In qualitative risk appetite statements financial institutions outline the levels and types of risk that they are willing to assume within their risk capacity to achieve their strategic objectives and business plans. Qualitative risk appetite statements can be broken down into two types: The first statement type refers to activities for which an institution has zero tolerance e.g., business relationships with sanctioned individuals or countries, restricted staff dealings in securities listed on an institution's restricted list, or any form of workplace harassment incl. discriminatory behavior against any staff members. Zero tolerance statements can be phrased positively (the bank is firmly committed to complying with all applicable sanctions regulations in every jurisdiction in which it operates) or negatively (the bank prohibits any business relations with sanctioned individuals, entities, or countries).

The second statement type refers to "restricted" activity that is generally still accepted but presents higher risk to the institution and is subject to mandatory approval requirements, enhanced monitoring, or other conditions (e.g., limitation of business volume). Examples include overdue customer complaints, a backlog of periodic know your customer reviews, and insufficient staff participation in mandatory training sessions.

2.2 KEY RISK INDICATORS

Key risk indicators are defined to determine and measure restricted business or other operational activity and refer to specific properties of customers and products. For example, to mitigate financial crime risk specific business activity with customers associated to PEP's[3] or from high-risk jurisdictions is subject to 2nd line of defense approval and enhanced monitoring. Or training participation below a certain committed percentage value trigger dedicated measures committed by senior management to ensure training gaps are closed within short deadlines or, if unsuccessful, potential repercussions for the individuals involved.

2.3 QUANTITATIVE RISK THRESHOLDS

Quantitative risk thresholds limit the volume of restricted or monitored business or operational activity. Thresholds can be determined as percentage values of overall business volumes or as absolute numbers:

- Target ambition levels represent the long-term intended level of activity
- Trigger values result in remedial actions to bring down the restricted or monitored volumes of business or operational activity
- Limit values require immediate action within agreed deadlines.

As noted above, risk environments for banks will be more volatile going forward. Risk appetite frameworks, originally intended to provide stability in risk management, must be embedded in flexible governance models allowing for efficient adjustment of criteria, indicators, and metrics to adapt to new risk exposures stemming e.g., from digital transformations and evolving product portfolios.

3 The technology opportunity: Leveraging AI to optimize compliance controls

To what extent institutions can make use of AI to optimize compliance controls depends on their data pervasiveness and the maturity of existing technological capabilities, which vary between institutions. Generally speaking, digital transformations offer two clusters of opportunities to optimize 2nd line of defence (LoD) controls, both from an efficiency and effectiveness angle.

First, when business process steps are automated, controls can be integrated and automated. While in the past compliance controls were often manual and detective by nature, the trend moves clearly towards automated, preventive controls enabling the organization to react to irregularities much quicker, ideally before misconduct occurs or deficient processes are performed. Transactions with specific parameters are processed fully automated (straight through processing) while other transactions will be routed to an exception queue where, depending on the control, 1st LoD analysts or 2nd LoD compliance officers will pick up the transaction and validate/ perform the control. The level to which controls can be automated depends on the sophistication and complexity of the control steps: The simpler and more repetitive steps are, the easier they can be automated. Complex controls will require an increased level of manual intervention. Compliance functions need to have full transparency on digitiza-

[3] Politically exposed persons.

tion initiatives to be able to integrate and automate compliance controls where possible.

Second, by producing large volumes of customer, transaction, and product data, digitization opens the playing field for artificial intelligence ("AI"). When built on an adequate infrastructure or platform, AI can help boost effectiveness and efficiency. In the financial services industry, the deployment of AI has many potential faces, from a pure efficiency and cost savings perspective to supporting the creation new products and services and improving the customer experience. AI can also help to make compliance controls more effective by, simply speaking, creating links between data sets, or detecting patterns of uncommon behavior, explained in more detail in the two following examples.

In financial crime prevention, AI can be deployed to make negative news screening more effective: Robotic process automation is deployed to extract negative news data from news sources, natural language understanding technology translates the retrieved data into machine-readable models which can then be automatically matched against customer names. Case-based reasoning technology helps to rank matching results according to degree of similarity between customer name and source data. An effective combination of all three technologies lays the groundwork resulting in matching tables based on which human analysts can make final "matching" calls more effectively and efficiently.

In the prevention of market abusive securities trading, AI can be used to detect uncommon, suspicious transaction patterns. First, individual trading patterns are created based on the ranges, volumes, and frequencies of transactions by traders. Case-based reasoning technology can be programmed to take in the various transactions executed by a trader and build corresponding trading patterns resulting in a group of securities commonly being traded by that trader, as well as corresponding trading volumes and frequencies. Second, the same technology can monitor ongoing trading activity against defined trading patterns and detect outlier transactions not in line with established criteria i.e., types, volumes, and/ or frequencies of traded securities. The detected outlier transactions need to undergo assessments by independent subject matter experts to understand the intention and rationale of the trades and validate them against trading mandates.

As noted above, for AI to deliver the suggested upsides financial institution need to reconsider their existing IT infrastructure. Often enough, existing computing powers are not sufficient for the three major phases that applications need to successfully go through:

- Data pre-processing: Data collection, consolidation, and formatting, often via ETL layer (Extract, Transform, Load) to cater for consistent data sets required for AI applications to operate at full potential
- Training: Prior to operating in real-time production, AI applications need to be trained (using test data and test cases) for the intended use-cases to develop the required level of effectiveness and efficiency; training is critical to ensure the AI application is enabled to achieve better results than the previous, manual process, otherwise it will be difficult to justify the required implementation effort
- Deployment: AI applications sufficiently trained are put to production, either stand-alone or complementary to existing screening or surveillance solutions.

The required infrastructure can be realized by using on-premises computing capacity, with applications running and data stored on the institution's servers, cloud computing using one or multiple external computing and storage capacities via the internet, or a hybrid model with both on-premises and public cloud components. The decision for one of the options is fundamental and several factors need to be considered incl. cost (high AI workloads on public cloud can become expensive, while on-premises capacity not fully consumed also comes at a price), data gravity (data volumes will grow over time and switching between options is complex), the sensitivity of (customer) data processed, the existing maturity and capacity of the IT infrastructure, and the AI strategy of a financial institution.

4 Leaving the comfort zone: Preparing compliance functions for agile transformations

The digital transformation disrupts the way banks operate. Banks with a digital footprint work in a faster-paced environment where product development cycles are shorter and disruptions through innovative technology occur more frequently. This requires a shift away from traditional hierarchical organizations and waterfall approach based working styles, which have proved to be less flexible and effective under fast moving conditions.

Instead, organizations need to adapt to the new conditions by turning agile. In essence, agile organizations can quickly and efficiently reconfigure strategy, structure, processes, people, and technology to better focus on customer needs and value creation. Agile transformations impact the way compliance functions interact with the various bank departments, particularly with the 1st line of defence. For maximum effectiveness and efficiency, the following success factors should be considered by compliance functions.

4.1 TEAM STRUCTURES AND GOVERNANCE

Agile organizations organize people flexibly e.g., in tribes or lattices around topics and goals, less along static hierarchical levels. Once assumptions change or goals have been reached, team structures may quickly shift again. Over the years, many compliance functions got used to dedicated communication channels into the business, often with constant counterparts at the other end. In an agile environment, this is very likely to change. Communication and general interaction with the business will be more dynamic and likely subject to recurring change of communication counterparts. Staff in compliance functions need to internalize this fundamental change an adapt their own working assumptions and styles accordingly.

4.2 ITERATION AND DECISION CYCLES

In contrast to traditional, pre-planned project management settings agile decision making is based on rapid cycles of thinking and doing. The frequency of iterations and their clocking is much shorter. So will be the window of opportunity for the compliance function to effectively introduce requests, questions, or regulatory concerns.

Input from compliance functions e.g., into product development and other business initiatives will likely be required at an earlier stage in the process, more frequently, and less formalized. To succeed in these new circumstances compliance staff need to be flexible, react more quickly, and adapt to potentially changing circumstances. Compliance leaders need to prepare their teams for this new environment by creating sufficient awareness, allowing them to embrace the new "agile" culture.

4.3 TECHNOLOGY ENABLERS

Agile transformations require the introduction of new, real-time communication and work-management tools. How people work and they way they communicate with each other changes and digital workplaces and communication channels replace many physical, co-located, and on-site interactions. Compliance functions must have full transparency on communication channels, work management tools, and other compliance relevant technology in place and be able to access these when required. Again, this requires awareness on behalf of compliance staff and the willingness to integrate technological innovations into (conventional) day-to-day working habits.

5 The digital compliance officer: Future qualifications and skill profiles

The future qualification profile of a compliance officer for a global financial institution is impacted by three key factors.

First, regulatory expertise is foundational. Traditional regulatory topics include those which have long been under the regulatory spotlight e.g., financial crime compliance incl. fraud prevention, market and customer conduct, data protection, and regulatory compliance. Compliance officers must also be experts the (future) regulation of contemporary topics e.g., big data, advanced analytics, artificial intelligence, blockchain technology, digital assets such as crypto currency, internet of things

Second, people, communication, and organizational skills are essential. Compliance requires interaction with several internal and external stakeholders including senior management, the business, other control functions, internal and external audit, and supervisors. Even though compliance officers have a regulatory mandate, sustainable change and impact requires the buy-in of these stakeholders. Third, to succeed in a digital world, a degree of technology affinity is helpful if not mandatory. Data and technology play an ever more dominant role e.g., in financial crime prevention where controls depend heavily on customer and transaction data and are executed automatically using monitoring, screening, and case management applications. Artificial intelligence comes into play more and more to help institutions optimize the efficiency of their automated monitoring and screening efforts. Only candidates with a thorough understanding of an institution's systems and data landscape will be able to connect the dots and deliver end-to-end impact.

6 The art of the possible: Cooperation as the next potential compliance trend?

Even though compliance in general and specific regimes such as the EU Market abuse regulation in particular aim to protect the integrity of financial markets most compliance efforts today are constrained to the boundaries of individual institutions. Many institutions, much like siloes lined up next to each other, are fighting a lonely fight in ensuring to comply with regulatory requirements and putting in place effective controls to mitigate Compliance risk. Undoubtedly, there is much interaction between the institutions, but very often that is restricted to an unbinding exchange of views and best practice sharing overshadowed by the fear of disclosing confidential information– the idea of swarm intelligence, or even Compliance cooperation between financial institutions is still underdeveloped in the industry. But, initiatives are ramping up with the intention to realize inter-institutional synergies, two examples of which are described below.

6.1 TRANSACTION MONITORING NETHERLANDS

The limitation of banks individually looking for money laundering and terrorist financing transaction patterns has been widely recognized, as criminals will often spread their transactions across multiple banks. Yet today, transaction monitoring is still a "lonely" game for most institutions. Transaction monitoring Netherlands (TMNL) however, set up in July 2020, is an initiative by five Dutch banks aimed at bringing together customer and transaction data transaction data from the different institutions and making meaningful connections between them through enhanced capabilities to analyze networks, patterns, and typologies across "boundaries" of individual banks. The links generated by TMNL using an integrated, cross-institutional transaction monitoring approach provide new insights into possible money laundering and terrorist financing and enable the institutions to detect potentially unusual transactions and new criminal patterns that would otherwise not be noticed. However, the integration comes at an effort: Before customer data can be centrally processed by TMNL it needs to be pseudonymized to cater for data protection requirements.

In addition to enhanced effectiveness, efficiency gains can be realized based on the centralization of monitoring activities freeing up scattered KYC efforts across individual banks. TMNL also makes a positive contribution the Dutch financial intelligence unit and investigative authorities as the quality of suspicious activity reports based on integrated transaction monitoring is expected to rise. Hence, financial crime can be tackled more effectively, giving criminals less room to operate.

6.2 KYC (KNOW YOUR CUSTOMER) UTILITIES

The concept of KYC utilities is to realize synergies by taking an integrated approach to data collection and data refresh efforts currently undertaken separately by individual institutions. Most banks suffer (to different degrees) from resource intensive, fragmented, and often highly manual KYC processes. Customers, on the other hand, often complain about multiple data requests and lengthy procedures, and an overall uneven, seemingly arbitrary KYC standard across institutions and geographies.

The range of potential utility solutions is broad, and so is the bandwidth of the maturity, market acceptance, and technical sophistication of existing concepts. However, the following advantages are common to most of them:

- Integrated collection of KYC data, preventing customers from providing data to multiple banks separately and recurringly
- Centralized storage of KYC data, under harmonized data standard
- Ongoing monitoring and refreshing of KYC data
- Enhanced customer control and easier access to up-to-date KYC data

KYC utilities offer key benefits both to participating financial institutions (centralized, convenient access to high quality KYC data) and their customers (simplified provision of KYC data and enhanced control over data). In practice however, KYC utilities are confronted with several operational challenges, including cross-jurisdictional constraints on data sharing, technical complexity resulting e.g., from the integration of external corporate or beneficial owner registries, the need to take precautionary measures against heightened risk from cyber-attacks, and lust but not least, required regulatory approvals (on behalf of the participating banks outsourcing the collection of KYC data to the utility). These factors can slow down market penetration and commercial traction.

7 Conclusion

To profit from digital transformations and keep risk oversight as effective as possible compliance functions need to prepare for the (substantial) changes that come with it. This requires awareness and an understanding of the changes at the horizon and how they impact day-to-day compliance operations. It is a key responsibility of senior compliance leaders to create awareness and understanding and enable their team members to embrace the challenge and develop the proper mindset to embark on a digital transformation. People's mindsets i.e., thought patterns are crucial as they determine how they will react to changes and behave in their (new) working environment. In the present context, mindsets can be created by a common compliance vision, or purpose and will help compliance officers to identify with the benefits of digitization.

ANSPRECHPARTNER:

Andreas Müller, KfW Bankengruppe,
andreas.mueller@kfw.de

Dr. Bernhard Gehra, The Boston Consulting Group,
gehra.bernhard@bcg.com

Norbert Gittfried, The Boston Consulting Group,
gittfried.norbert@bcg.com

Dr. Georg Lienke, The Boston Consulting Group,
lienke.georg@bcg.com