New Anti-Money Laundering Requirements in the UAE: How Banks Can Adapt

White Paper · April 2022

BCG

The agenda

The authors

Norbert Gittfried

Norbert Gittfried is a Partner & Director based in Central Europe

Gittfried.Norbert@bcg.com

Dr. Bernhard Gehra

Bernhard Gehra is a Managing Director & Senior Partner based in Central Europe

Gehra.Bernhard@bcg.com

Felix Hildebrand

Felix Hildebrand is a Partner active in Central Europe and the Middle East

Hildebrand.Felix@bcg.com

Aytech Pseunokov

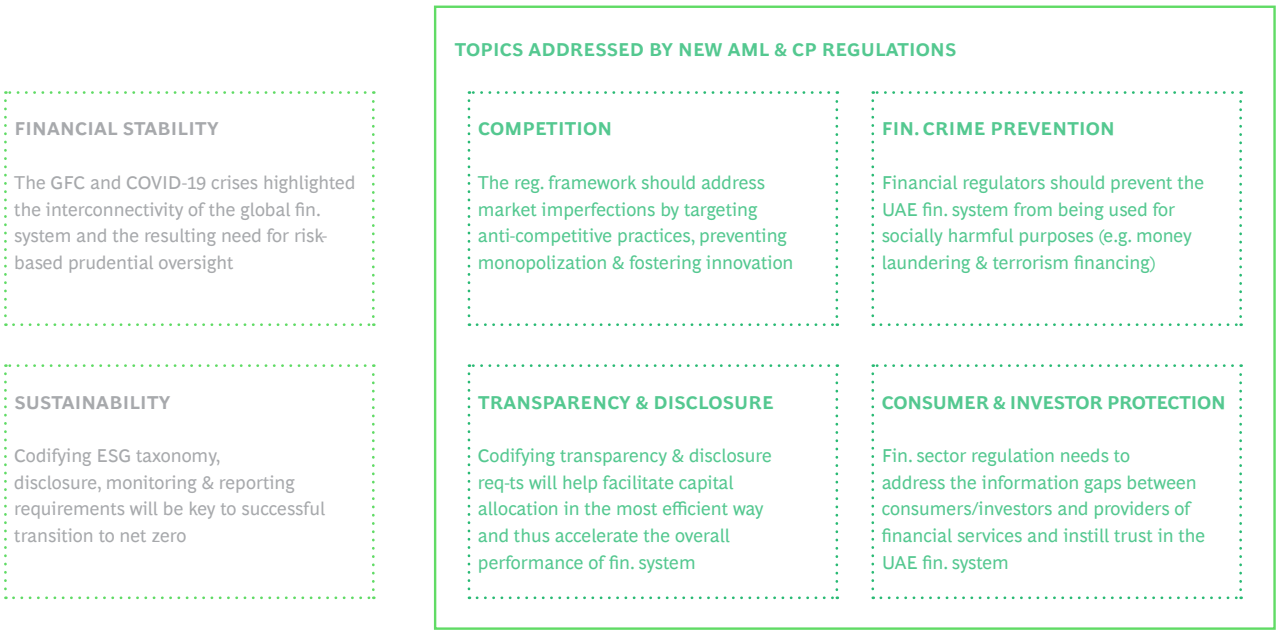
Aytech Pseunokov is a Project Leader based in the Middle East

Pseunokov.Aytech@bcg.com

Introduction

In 2021, the Central Bank of the UAE (CBUAE) published several regulations and standards for the banking sector. These encompass several key areas of financial regulation, including anti-money laundering (AML), consumer protection (CP), and data security *(see Exhibit 1)*. Some of the new anti-money laundering requirements present significant operational challenges. In order to comply, some banks may need to revise their transaction monitoring (TM) systems and compliance organizations. Still, with the right approach, they can design resilient, future-proof compliance target operating models that meet or exceed regulatory expectations.

EXHIBIT 1. CBUAE AML & Consumer Protection regulations address 4 of 6 key areas of financial regulation



The AML & Combating the Financing of Terrorism (CTF) landscape is seeing rapid change, with the CBUAE actively strengthening its regulatory framework and bolstering its oversight activities, also following the outcome of the 2020 Financial Action Task Force (FATF) mutual evaluation. We should therefore expect the UAE to take further action to address identified topics and comply with the FATF Recommendations.

The CBUAE has already shown that it will not hesitate to enforce its AML requirements. Indeed, it has imposed fines totaling more than AED82 million (US$22.48 million) on 12 banks[1] and 6 exchange houses[2] since the beginning of 2021. At the time of writing, the most recently published was a fine of AED19.5 million imposed on a local bank for AML failures[3].

1 "CBUAE imposes financial sanctions on 11 banks operating in the UAE"; "CBUAE imposes monitoring and financial sanctions on a bank operating in the UAE"
2 "CBUAE imposes financial sanctions on six exchange houses"
3 "CBUAE imposes monitoring and financial sanctions on a bank operating in the UAE"

These financial penalties, while still relatively small compared with those in the US and EU[4], send a clear signal to the UAE financial services industry that compliance failures will not be tolerated.

Another area of regulatory activity has focused on consumer protection and data security. The central bank's Consumer Protection Regulation and accompanying Standards apply to all UAE-licensed banks and cover topics including data protection, governance, ethical conduct, and financial inclusion and awareness. Data protection in particular is emerging as a new challenge for compliance functions, and certain provisions of these regulations and standards may also have an impact on AML compliance programs.

Key Challenges of the New Regulations

Over three months from June to September 2021, the CBUAE published or updated at least six different guidelines on AML topics applicable to banks, including:

1. **Updated Guidelines** for Financial Institutions on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations, June 2021;
2. **AMLCFT[5] Guidance** for LFIs[6] on Suspicious Transaction Reporting, June 7, 2021;
3. **AMLCFT Guidance** for LFIs Providing Services to Legal Persons and Arrangements, June 7, 2021;
4. **AMLCFT Guidance** for LFIs Providing Services to Real Estate and Precious Metals & Stones Sectors, June 16, 2021;
5. **AMLCFT Guidance** for LFIs on Transaction Monitoring and Sanctions Screening, September 8, 2021; and
6. **AMLCFT Guidance** for LFIs providing Services to Cash-Intensive Businesses, September 27, 2021.

The guidelines provide additional clarity on the preferred risk-based approach and standards expected of bank AML and sanctions programs. However, they also introduce new requirements, some of which may present substantial operational challenges.

4 SEB Bank fined $107 million for AML failures
5 Anti-Money Laundering and Countering the Financing of Terrorism
6 Licensed Financial Institutions

One of the most notable changes was brought about by CBUAE Guidance on Suspicious Transaction Reporting. The Guidance introduced a requirement to file suspicious activity/transaction reports within 35 days of a first alert (including 20 days for analyzing the alert and making a decision on whether it warrants an STR/SAR filing, and an additional 15 days for preparing and filing the STR/SAR)[7]. To many banks, this presents the prospect of a difficult transition, which may require a full revision of the AML compliance organization and, more specifically, transaction monitoring and screening frameworks.

Automation and a Resource-driven Approach

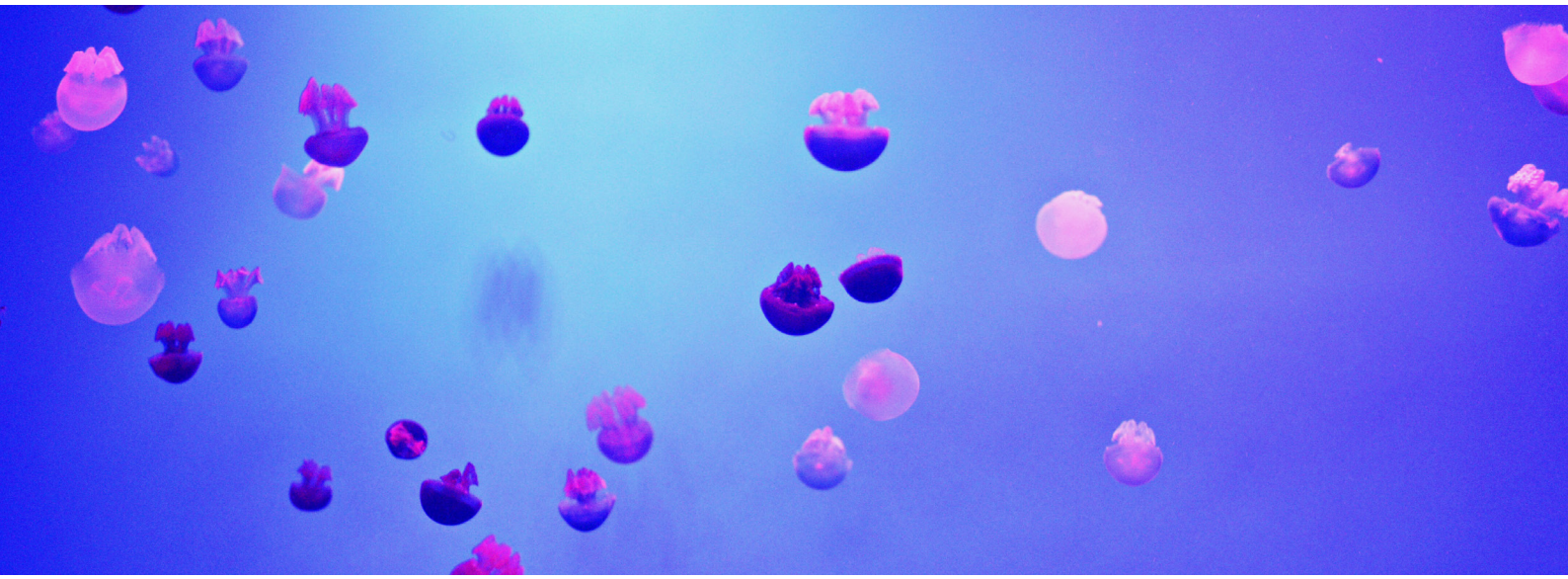
Changing or upgrading a transaction monitoring system may take years whereas the CBUAE gave banks a grace period of one month to comply with the Guidance on Suspicious Transaction Reporting (including the 35-day SAR/STR filing rule). To many banks, especially those that use fewer automated solutions for transaction monitoring, a natural short-term solution may be to hire additional staff to increase the speed of processing SAR/STR alerts. However, there are challenges associated with this approach.

First, any transaction monitoring system lacking automated solutions is likely to be ill-suited to the fintech revolution already underway in the UAE financial sector. With fintech solutions and digital distribution channels positioned to deepen their banking penetration[8], the number of banking transactions is likely to rise. In the absence of advanced technology solutions for automated detection and analysis of SAR/STRs, these trends are likely to result in a growing number of STR/SAR alerts, creating an ever-increasing demand for compliance resources. Coupled with the CBUAE requirement to avoid defensive filing[9], banks must strike a delicate balance between maintaining a team of professionals sufficiently qualified to process and escalate alerts (to the satisfaction of the CBUAE) and managing budgets and risks associated with hiring more compliance staff. The CBUAE itself has emphasized that the effectiveness of manual analysis is undermined by the complex and evolving nature of financial crime risks.[10]

There is another reason why simply hiring additional staff for manual alert processing in lieu of automation may not be the best approach in the longer term. Traditionally, the primary cost-benefit of this approach was derived from relocating or outsourcing operational tasks (such as level 1 alert analysis) to offshore locations with a lower cost of labor. However, other regulatory changes introduced by the CBUAE may restrict cross-border transfers of data out of the UAE, prompting banks to reconsider the benefits – and risks – associated with offshoring.

7 Article 4.6 of the AMLCFT Guidance for LFIs on Suspicious Transaction Reporting
8 Source: CBUAE Financial Stability Report 2020
9 Article 3.3.1 of the Guidance for LFIs on Suspicious Transaction Reporting
10 Article 2.6.1 of the Guidance for LFIs on Suspicious Transaction Reporting

Regulatory Implications of Offshoring and Outsourcing



In 2021, the CBUAE issued several regulations and procedures that had a direct impact on offshoring arrangements, including:

- **The Consumer Protection Regulation (CPR) and accompanying Standards (CPS)**
- **The Outsourcing Regulation for Banks (ORB) and accompanying Standards (OSB)**

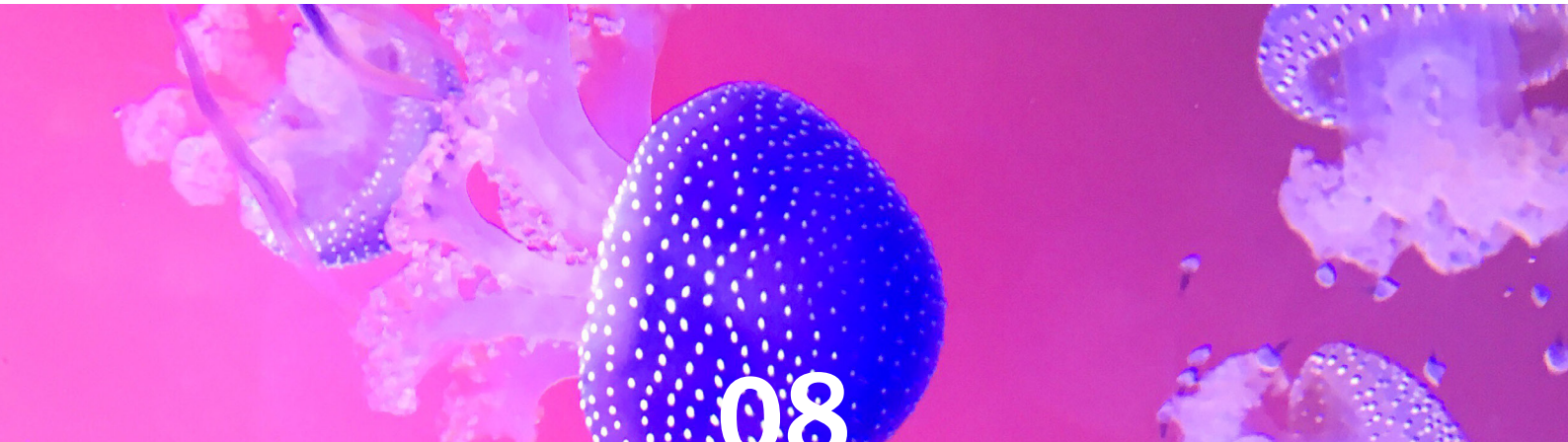
While these impose a variety of requirements, we here focus on those that may have implications for offshoring or outsourcing compliance tasks to another country:

1 **Cross-border data transfers/processing.** The CPS contains a requirement that banks store all of their customer and transaction data locally in the UAE (article 6.1.6.3). At the same time, article 6.3 of the ORB implies that it may be possible to share such data outside of the country for outsourcing purposes, subject to CBUAE approval and written consents of customers whose data is being shared. However, ORB prohibits outsourcing into jurisdictions that cannot provide the same level of protection of personal data as the UAE. Drawing a parallel with the EU GDPR, the CBUAE data protection regime may be considered at least as strict, after the landmark Schrems II CJEU ruling, which limits the conditions on which personal data may be transferred and processed outside of the EU. It also remains to be seen whether, and how, the CBUAE data transfer provisions are affected by the new UAE data protection regulations, expected to be published in 2022.

2 **Cyber security & governance.** Under the CRP and CPS, banks must ensure the security of all customer data they collect, including preventing misuse, use for financial crime, and misappropriation. Upon discovering breaches, banks should log them, notify the customers affected, and compensate for any damages resulting from the breaches. Banks must also notify the central bank of any "material" data breach, loss, destruction, or alteration of data when they occur. Satisfying these requirements becomes more complicated when incidents occur outside the country and can be further complicated if a third-party provider is involved. In this case, the bank would need to mirror its liability to customers in its contractual arrangement with the third party and consider the risks associated with enforcing such a contract in a third country. In addition, article 11.3 of the ORB implies that the CBUAE may require a bank to terminate outsourcing agreements that present "undue risks" to data protection.

3 **Written disclosure and consent requirements.** Article 6.3 of the ORB states that confidential customer data must not be shared outside the UAE without the approval from the CBUAE and prior written consent from the customer, together with a written acknowledgment that her/his confidential data may be accessed under legal proceedings outside the UAE. CPR and CPS also state that before disclosing a customer's personal information to any third parties, the bank must inform the customer of how exactly her/his data will be processed and obtain her/his express consent for such disclosure. It is important to note that such consent may be withdrawn by the customer at any time during which the personal data is being processed by the financial institution or shared with a third party, in which case the financial institution has 30 calendar days to complete the withdrawal request. This presents an additional challenge in the context of offshoring because the bank must convey the requests to its offshore location or the third party providing the services and ensure they are completed.

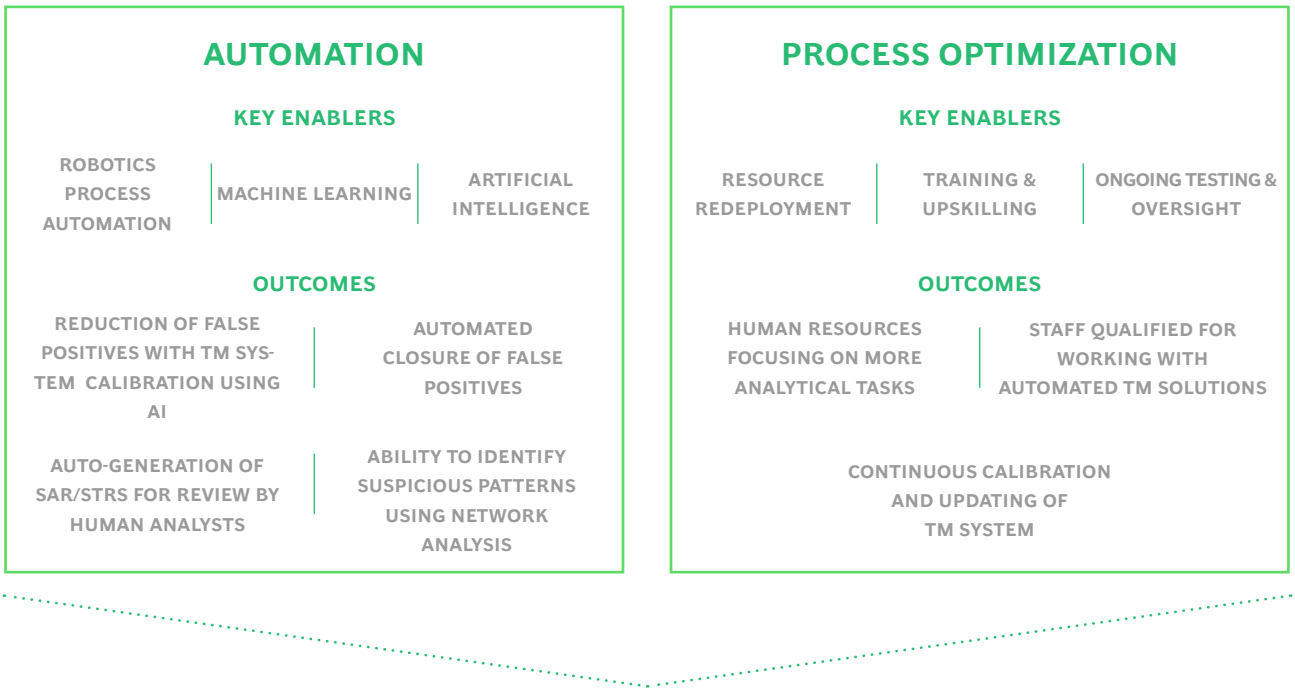
It remains to be seen how these requirements will impact offshoring arrangements for operational compliance tasks such as SAR/STR alert reviews. There may still be alternative solutions (e.g., offshore staff working remotely through the cloud on data physically stored in the UAE). However, the key question would be whether such solutions are justified from an effectiveness and efficiency viewpoint, considering the associated HR, operational, and regulatory risks.



Automation and Process Optimization: Key Elements of a Successful Transaction Monitoring Program

An alternative solution for meeting the new CBUAE alert handling timelines would be taking a two-pronged approach, combining automation and process optimization. *(See Exhibit 2).*

EXHIBIT 2. Combined approach to reduce alert investigation timeline



Gradual, carefully-planned implementation of Machine Learning (ML), artificial intelligence (AI), and Robotics Process Automation (RPA) will be increasingly critical to tackling the AML challenges of tomorrow. The CBUAE acknowledges this fact in its Guidance on Transaction Monitoring and Sanctions Screening, making it clear that it expects larger financial institutions to put automated transaction monitoring systems in place.[11]

11 Article 2.2 of the Guidance for LFIs on Suspicious Transaction Reporting

Initial deployment of automated tools for alert analysis requires a certain pre-existing level of digitization readiness and usable data, as well as senior management support. However, if implemented effectively, it has the potential to dramatically shorten alert handling timelines and reduce false positives. Below we gather four of the many possible use cases for automation in TM:

1 **Calibration of TM systems.** A common way to finetune TM systems is above-the-line/below-the-line testing. This is a statistical method of finding the optimal balance between reducing the rate of false positives and improving the effectiveness of detection of suspicious activities and generation of SAR/STR alerts (by changing predetermined thresholds in the TM system). To increase the effectiveness of this type of calibration, AI can be deployed to segment customers and products based on their risk profiles. Performing above-the-line/below-the-line testing individually in each category helps improve the overall accuracy of alert generation.

2 **Auto-closure/escalation of alerts.** RPA can be implemented to analyze alerts and automatically close those with a true positive likelihood below a certain threshold (e.g., less than 5%). At the same time, alerts meeting the true positive criteria with higher probability (e.g., more than 90%) could be directly escalated for level 2 analysis and preparation of STR/SAR filings.

3 **Alert hibernation.** This is the process of saving for future review alerts that by themselves do not necessarily warrant escalation but may raise suspicion if repeated a certain number of times. Using RPA, TM systems can be programmed to hibernate low-risk alerts instead of closing them altogether and to escalate them to a human investigator if a repeated alert is generated on the same customer or account, indicating potentially suspicious activity.

4 **Pre-evaluation of alerts.** An "RPA bot" can be deployed for automated research and information gathering on alerts escalated for manual review. By some estimates, this type of work accounts for ~75% of level 1 alert investigation efforts[12]. In addition, banks can deploy supervised ML to analyze decisions made by humans on similar transactions. After several months of continuous training (depending on the amount of historical data on past alert reviews), the ML solution would be able to generate recommendations on the steps to be performed by the analyst to review the alert, based on past reviews of similar alerts. The analyst would still need to review the recommendations and either confirm or reject them. However, every new decision would train the ML algorithm and improve its accuracy.

12 BCG estimate based on project experience

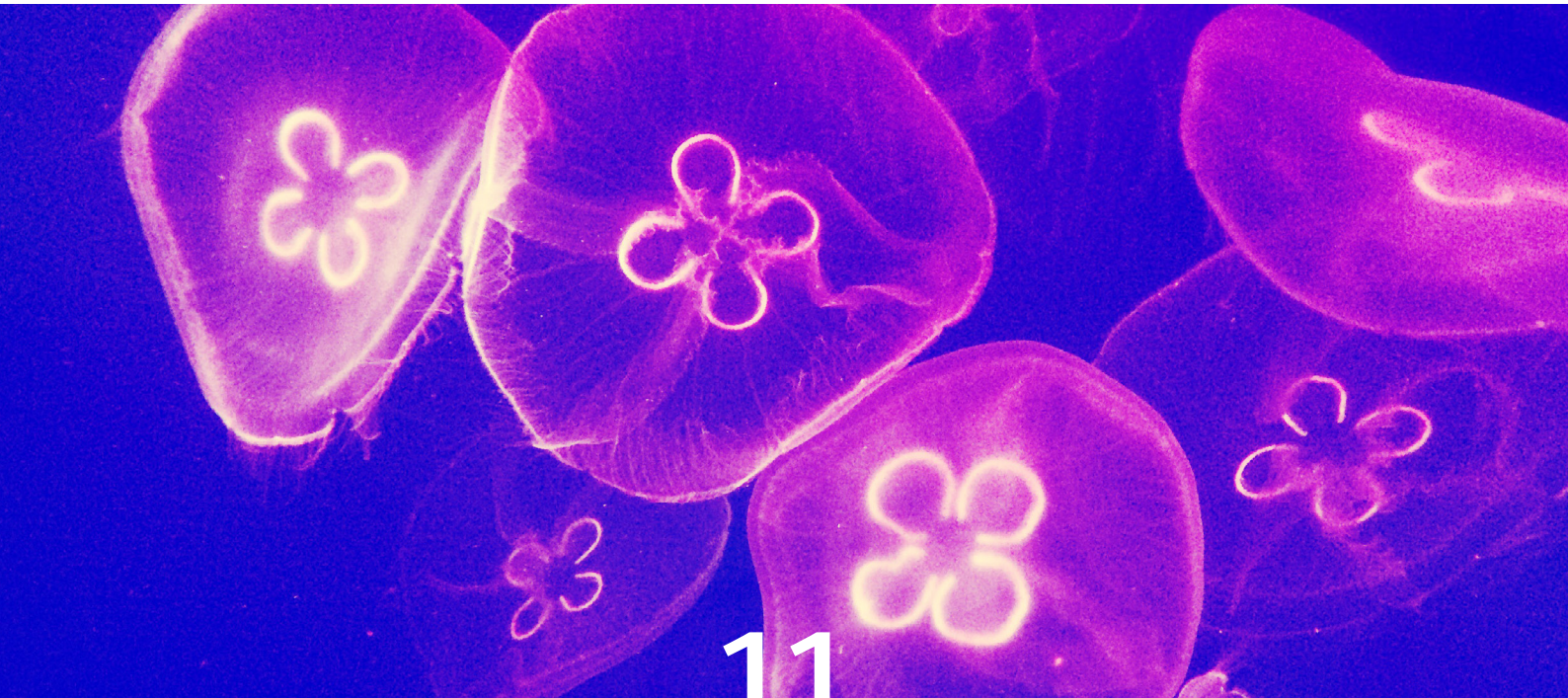
While RPA, ML, and AI-powered solutions present numerous operational opportunities, one flip side is their lack of transparency. All decisions are made in a “black box” and are not immediately visible to human observers. This lack of clarity should be addressed by documenting the processes and procedures for setting and calibrating the rules, thresholds, and filters used by the automated TM system, and fully aligning them with AML policies and procedures, as well as regulatory requirements.

It would also be a mistake to think that automation implies the elimination of human resources. Banks require qualified staff with sufficient levels of expertise to work with, maintain, and periodically test TM systems, as well as to carry out regular reporting to senior management in line with CBUAE requirements. Continuous targeted staff training and upskilling will be key to the success of an automated TM program.

In summary, when implemented effectively, automation of TM systems, coupled with process optimization, can help unlock the following key benefits:

1. **Increased effectiveness** of the TM system through enhanced ability to detect suspicious patterns via AI segmentation and network analysis, as well as reduction of false positives through AI-enhanced calibration.

2. **Increased efficiency,** comprising automated closure of false positives coupled with the direct escalation of likely true matches, as well as RPA-powered automatic collection of supporting data. This will reduce alert handling times and free up compliance resources, which can then be redeployed for speedier handling of alerts with the same FTE resources.



Roadmap to Compliance

When comparing compliance approaches to individual regulations, the temptation is to opt for the quickest and simplest solution that checks all the regulatory boxes (at least for the time being). This is particularly the case given the tight implementation deadlines typically set by regulators. However, quick solutions often do not withstand the test of time and run the risk of eventually crumbling under the weight of ever-increasing regulatory demands. As we have seen, a TM system lacking automation tools for alert detection and analysis will be much more difficult to maintain in the longer term if the banks' customer base and transaction volumes continue to increase.

For a bank to deploy state-of-the-art automation solutions, it will need robust planning, cross-functional coordination, and the necessary compliance organization to undertake project management. The effectiveness of any TM system (even the most advanced) will depend on the operating environment in which it is maintained. A good compliance operating model should serve as a backbone for regulatory adaptations, and this should take into account not just immediate CBUAE requirements but also the key objectives and overall direction of regulatory policy and industry trends, both in the UAE and globally. Once the system is built and implemented, any future regulatory adjustments become much easier to implement in a relatively short time frame.

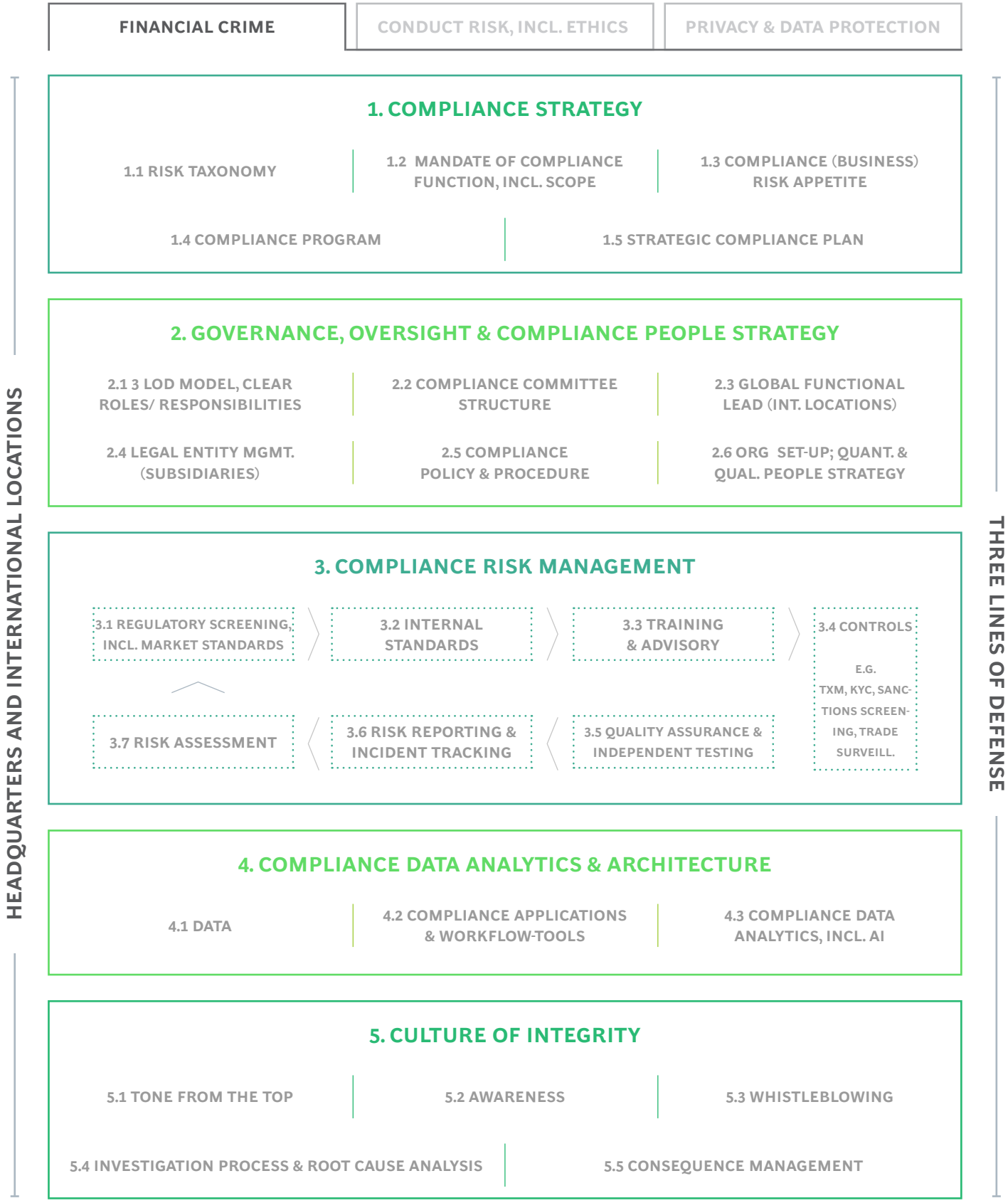
With the right amount of effort, a compliance TOM can be built in three stages:

STAGE 1. The starting point is a holistic "health check" of the current compliance operating model across five key dimensions:

- **Compliance strategy**
- **Governance, oversight, and people strategy**
- **Compliance risk management**
- **Compliance data analytics and architecture**
- **Culture of integrity**

The TOM design in *Exhibit 3* provides a reference for the structure of key assessment components. The recent CBUAE regulatory developments cut across all five dimensions. However, a comprehensive diagnostic test would also highlight other areas of the compliance organization requiring attention, beyond those impacted by the regulations.

EXHIBIT 3.
BCG's Compliance Target Operating Model design



STAGE 2.

If any gaps are found, banks should undertake a qualitative assessment to identify underlying reasons and elements necessary to close the gaps. For example, if the bank is storing data in several different IT systems, there is a case for creating an integration layer for feeding data from those systems into a screening tool. The CBUAE encourages banks and LFIs to review their TM programs at least annually.[13]

STAGE 3.

Once the required remediation actions are defined, the final step should be to prepare an implementation roadmap detailing the time and resources required to build the target operating model.

As the pace of regulatory change accelerates, banks in the UAE need to learn quickly how to adapt to new requirements. The trend is likely to continue, not least because the CBUAE is facing emerging AML challenges. Having reviewed different approaches to addressing the new suspicious-activity reporting requirements, we conclude that automation, coupled with process optimization, presents a potentially effective combination for reducing alert handling timelines and future-proofing AML TM systems. However, these cannot be implemented without a forward-looking target operating model, which should serve as a foundation on which an effective AML program can be built. The roadmap described here should provide a useful reference for addressing immediate challenges and building a solid base on which to prepare for the regulatory challenges to come.

13 Article 2.6.2 of the Guidance for LFIs on Suspicious Activity Reporting

About BCG

Boston Consulting Group is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not- for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with offices in more than 90 cities in 50 countries. For more information, please visit bcg.com.

BCG

www.bcg.com