AML/CFT DIGITAL STRATEGY FOR LAW ENFORCEMENT AUTHORITIES

MAY 2022

Technology is transforming the financial services industry, including through wider and quicker access to services that are no longer bound by geographical boundaries. At the same time, it is transforming the way criminals, terrorist financiers, and sanctioned individuals raise, move, or layer funds to finance and disguise illegal activities such as online fraud, ransomware attacks or sanctions evasion.

The response to these threats is also evolving. In recent years, law enforcement agencies have built up their digital capabilities to exploit the immense potential of a data-driven anti-money laundering and counter terrorist financing (AML/CFT) strategy. Technologies such as automation, blockchain analytics, big data, artificial intelligence (AI), machine learning and other advanced analytics can help authorities investigate money laundering (ML) and terrorist financing (TF), assess risks, and exchange information within the public sector and with the private sector.

In May 2022, the Financial Action Task Force (FATF) prepared a confidential report that explores how law enforcement agencies can use technology to successfully investigate money laundering and terrorist financing, mitigate the risks of these crimes and share information in a secure manner. The report highlights the opportunities, requirements as well as the key prerequisites for removing the barriers to successful digital transformation. This document focuses on the key strategic questions to be considered prior to launching digital initiatives.

OVERALL STRATEGIC CONSIDERATIONS

It is important for the senior management to understand the problems faced by the law enforcement authorities before embarking on their digital transformation journey. Below are some suggested key strategic questions that should be considered:

- Is there a problem statement to guide the agency in understanding the priority and common goal(s) of the project? For example, the project statement can consider questions such as the following: does the agency need to speed up certain type(s) of investigations, or is the agency having difficulty in uncovering wider criminal networks?
- Is there an aligned vison among internal key stakeholders (from leadership to frontline investigators) and a shared understanding within the agency about the objectives and business case of the digital initiatives? While stakeholders may agree with the need for digital transformation, they may have different mid- and long-term priorities and interests, available resources and capabilities, and organisational limitations. To allow a successful national strategy of digital transformation for AML/CFT, considerations of how to secure buy-in from different stakeholders would be required.
- Is the agency clear about how digital tools can extract most value from existing data/intelligence?
- Is there a clear implementation roadmap that is matched with necessary resources and requirements (including expertise, finance, processes, data, technology, etc.)?
- Has the strategy considered and identified any quick-wins as a proof-of-concept, possibilities to jump-start with an impactful deliverable, or essential building blocks for scaling-up, and prepared for adjustment along the way based on review?
- Has the strategy built in a regular review mechanism such that users feedback can be incorporated in future updates of the implementation strategy?
- Are there adequate in-house technological and programme management capabilities or trusted third-party partners to oversee and support the delivery of the programme?
- Does the agency have sufficient standardised data to support digital transformation? If not, is there a plan to develop data readiness within the agency?
- Does the agency have the right set of technical skills to integrate digital tools into the investigative workflows? If not, is there a training and/or procurement strategy in place to support the implementation of the initiative?

- Are organisational or structural changes required to implement the initiative – for example setting up a specialised unit, or a complete reorganisation?
- Has the impact on operational processes communicated to affected staff, and whether measures are in place to ensure the agency to be digital-ready?

SPECIFIC LEGAL AND ETHICAL CONSIDERATIONS

Once integrated, standardised, and analysed, the data/information collected can be very useful in detecting and identifying suspicious activities, patterns, parties and associations for assessments, intelligence and investigative purposes. Nonetheless, it is crucial for law enforcement authorities to be mindful of the following considerations to ensure legal, responsible, ethical use of the data/information collected. This will also allow building trust and confidence in the digital transformation initiatives.

- Is the implementation roadmap aligned with existing and foreseeable data protection, privacy, and security frameworks and legislation? Are amendments to existing legislation needed to allow the use of technologies such as machine learning and big data analytics?
- Does the agency have robust understanding and governance regarding its legal framework? This will provide a solid foundation to understanding the rules respecting search and seizure, privacy protections, disclosure, admissibility of evidence, etc.
- What are the legal considerations on the application of AI, machine learning and advanced analytics when using various data sources (in-house, third party, and open source data)? This is important as an effort to avoid negatively impacting privacy issues.
- Will the use of emerging or advanced technology bring ethical considerations? For example, is it ethical to monitor one's own population with AI? What are the data privacy implications for a potentially wider scope of inspection and extraction that could be supported by new technologies? Agencies should carefully consider the method for obtaining vast amount of "private and regulatory" information for criminal investigations with a view to avoiding any perceptual or real "misconduct" allegations.

OTHER KEY STRATEGIC QUESTIONS

DIGITAL INITIATIVES SUPPORTING ML/TF INVESTIGATIONS

- Which specific types of ML/TF crimes would benefit most from the use of technology?
  - Should it be based on national priorities, country risk profile, threat or impact of such crimes?
  - Should the agency pilot or begin with the readily available datasets (such as company registration or beneficial ownership information) and those in an already structured format?
  - Should the nature of crimes cast a determining factor in requiring a digital approach to investigation? For example, crimes facilitated by new technologies (such as virtual assets), or crimes that are data-intensive (such as trade-based money laundering).
- Which specific digital investigative capabilities are considered as "core competencies" and should be developed in-house?
- Are there any third-party tools or services that deliver reliable and quality results, and that the agency will not need to replicate such competencies internally and focus on appropriate procurement? For example, digital forensics or blockchain analytics.
- If the key types of ML/TF crimes faced by the jurisdiction is cash-intensive and in the informal sectors, how to improve data and system readiness?
- How often should the system be validated as part of the development, and on what specific criteria? What external validation can be used to ensure the systems/ models used continue to support evolving trends and needs of ML/TF investigation?

MORE INFORMATION

SCAN ME

www.fatf-gafi.org

DIGITAL INITIATIVES SUPPORTING
RISK ASSESSMENT

- How will the data be "sanitised" to remove potential bias and inaccuracy?
- What are the known limitations of the risk models that may affect findings? Do they accurately reflect the risks, or reflect biases of investigators / known findings / existing prosecution results?
- How often should risk models be validated or verified and on what specific criteria? What external validation can be used to ensure the models continue to reflect evolving risks in reality?
- Is there a training dataset that the risk modelling (or artificial intelligence model) can learn from? Is the agency expecting such model to calibrate or replicate existing human analysis, existing court judgements, or to identify patterns that investigators would/could not otherwise?
- How will the risk assessment tool be updated to reflect secular or structural changes? For example, the impact of COVID-pandemic on legitimate spending patterns, the emergence of virtual assets, etc.

DIGITAL INITIATIVES SUPPORTING
INFORMATION EXCHANGE

- Has the initiative identified key components of data to be shared, and why such sharing is in line with the national AML/CFT priorities and risk profile of the country?
- Is the data to be shared available in compatible data format or structure, and will not require substantive cleaning and harmonisation efforts?
- Is there a plan to verify data accuracy, or to obtain updated data to increase the relevance and value of the shared data?
- Do stakeholders (both public and private) understand the strategic importance of the proposed information exchange and be committed in working in a collaborative manner?
- Is there a plan to build trust between private and public sectors, or between government agencies before initiating data transformation initiatives? For example, the agency may consider launching initiatives to standardise data format. The availability of more complete, accurate, and reliable datasets will also allow subsequent information exchange initiatives.