How to make financial crime prevention pay-off Implementation strategies to reap the benefits of the holistic model

Piero Molinario
Partner
Forensic & Dispute
Deloitte Italy

It is difficult to quantify the costs of financial crime-there is no doubt that it has become a significant issue for organisations and one that is more challenging by the day

Introduction

For over two hundred years, the world of academia has studied the relationship between economic business cycles and increases in crime.

Notwithstanding other aspects that may contribute to increases in criminal activity, the last economic recession has, undoubtedly as measured by the number of enforcement actions reported in the media, accelerated the quest to uncover criminal activity, ranging from fraud and corruption to money laundering and tax evasion.

In this respect, the recent economic crisis has been something of a turning point in the regulatory response to financial crime around the world. The failure of light-handed regulation and risk assessment by both the private sector and regulators has significantly changed the landscape in terms of expectations and ways and means to address them.

In this article, we discuss implementation strategies that, based on lessons learned, have enabled organisations to gain the benefits promised by the ever more prevalent consolidated approach to white-collar crime prevention.

The inescapable pressures of tackling financial crime

Arguably, legislators, regulatory bodies and enforcement authorities have long deputised the private sector in the global fight against financial crime. This is especially true for the financial service industry with respect to money laundering and terrorist financing but also for other industries with respect to corruption, bribery, fraud, tax evasion, insider trading and more. Over the years, the work of supranational standard setting bodies and of particularly rigorous legislators of countries such as the U.S., UK, Australia and more has created a fine-mesh net of international standards, laws with an extraterritorial reach and demanding domestic regulatory frameworks (e.g. FATF recommendations, USA PATRIOT Act, FCPA, UK Bribery Act, etc.) that have 'raised the bar' globally.

This evolution, characterised by an imperative to fight financial crime and the intense pressure brought about by governments' enforcement actions around the world, has increased the cost of doing business. In parallel, the private sector has increased its focus on risk management and thus, among other things, on proactively trying to weed out illegitimate and illicit activity to manage the risk and implications of non-compliance and to preserve reputation.

This convergence has created a very interesting environment where not only governments but also the private sector is concerned with financial crime prevention. Not surprisingly, the higher level of scrutiny and expectations in relation to financial crime and risk management has become a stay-awake issue for corporate directors and senior management around the world, who are seeing an increased expectation, both internally and externally, for compliance programmes that are effective at addressing risk. Consequently, effective compliance has become central to achieving business strategy. While it is difficult to quantify the costs of financial crime—which can include direct losses, record-breaking fines for non-compliance, penal actions against individuals, lawsuits and reputational damage—there is no doubt that it has become a significant issue for organisations and one that is more challenging by the day.

Over the last decade, organisations have made significant investments to be compliant with anti-money laundering, anti-bribery and corruption and anti-tax evasion laws and regulations. In the beginning, many organisations were more reactive, often implementing policies, procedures and controls in response to regulatory requirements that were more prescriptive in nature. Generally, organisations were fighting financial crime in silos (e.g. with an AML department, a Fraud Investigation Unit, etc.), and within those, they were focusing on the compliance chores or processes stemming from the regulations (e.g. client onboarding, transaction monitoring and reporting, vendor screening). In a quest to manage their risk exposures more effectively while containing the ballooning cost of compliance, many organisations began to view financial crime in a more holistic way.

The case for moving from a fragmented to an integrated approach

As crimes continue to increase in subtlety and sophistication, and may appear to discrete detection processes and intelligence systems as a set of unconnected and potentially normal activities and behaviours, merging unconnected financial crime programmes is the only way that organisations can build an accurate defence mechanism.

Without an integrated approach, firms will likely continue to invest in activities that simply do not provide the flexibility to keep up with changes in the regulatory landscape or the increase in sophistication and creativity of the more nimble criminals. With no way of joining the dots in their data, the effectiveness of the risk management will eventually degrade. Firms that fail to improve or at least maintain effective measures against financial crime are likely to suffer greater financial loss and reputational harm, and organisations and their employees will be left more vulnerable to punitive action by the regulators.

With a legacy of desperate approaches to contend with and increasing cost pressures, organisations could easily choose a path of minimal compliance. Before they take this line though, they should consider whether an integrated approach, centred on bringing their data and analytics together, would help improve the quality of their financial crime prevention efforts while simultaneously reducing costs.

Reaping the benefits of an integrated approach

A consolidated model to financial crime enables previously disconnected areas of financial crime prevention activity to be linked, in order to explore the overlaps, synergies and linkages that exist between cross-organisation processes and data sets. Said interconnections can then be used to build risk mitigating measures as well as models capable of estimating the probability of future crimes occurring, which means organisations can become proactive rather than reactive, and thereby reduce the potential for significant losses. Further, a centralised model allows managers to derive key performance indicators and timely and accurate management information, which can then be used for essential benchmarking and reporting, which in turn can increase quality and reduce cost.

Our Forensic partner Ivan Zasarsky at the Deloitte Australia office, provides us with insight on the benefits of a consolidated model: *'It seems that when alignment of managed interests become a priority, any number of unintended opportunities emerge. We have seen that when the adversaries (bad actors) conduct their operations … clearly, they do not play within a business unit or specified jurisdiction. When protection of the institution is everyone's responsibility, the engagement of key departmental and line of business leaders is essential. In my experience, the alignment of enterprise-wide financial crime productivity results in: reduction of duplication / redundancy (e.g. processes, applications, data, etc.); increased transparency of risk (e.g. more effective identification, management, mitigation, etc.) and heightened mindshare (e.g. culture shifts, enhancement of front line awareness, corridors of communication within and outside of the organisation, etc.).'*

How have organisations successfully transitioned from the pigeonholed approach so loved by the agile and flexible 'bad actors' which treated criminal activities as if they were separate and distinct (e.g. fraud from money laundering) to a consolidated view and approach to financial crime? It has not been without challenges, however, some have managed the transition and there are lessons to be learned. Following is an account of some key considerations that stem from our collective global and cross-functional experience.

Live by the findings of the enterprise-wide financial crime risk assessment

Rather than continuing to pump time and money into a patchwork of compliance chores and systems to tackle financial crime, organisations should start afresh, from an objective assessment of their risk profile. They should analyse, in detail and holistically, their exposure to financial crime risk. Doing so, with a methodical and repeatable approach, will not only identify, assess and quantify the present or eventual risk exposures (e.g. a subset of clients or services, a newly formed business or one expanding in a new market, a weaker procedure, etc.) but also the related mitigating measures currently in place (or not) in terms of policy, procedures, and controls. From the assessment of the risk exposures, mitigating measures and the resulting residual risk or 'gap' will stem an enterprise-wide risk assessment heat map that will serve as the starting point for the consolidated financial crime prevention strategy. From the latter, the organisation will then develop a target-operating model that aligns strategy, people, process, technology and data capabilities.

Set a resilient consolidated financial crime strategy

To effectively detect, assess, prevent and respond to financial crime, organisations need to design a strategy that takes a holistic view of financial crime risk as determined through the risk assessment findings and that is sufficiently agile. A static or reactive approach will likely fail, while a fragmented one is not enough. Institutions need to iterate their financial crime management strategy with the same commitment and effort as they would their corporate or customer strategy. They need to know where they are going to focus their efforts and how they will be successful in mitigating financial crime as a result of those efforts. Only then will it become clear that the fight is a joint effort that needs to be countered with common capabilities and systems.

Key aspects of resilient strategy often include:

- The overall organisation vision on how and why to combat financial crime
- The main pillars or themes for a consolidated fight against financial crime (leading rather than following the industry, risk assessment approach, tone from the top, leveraging all available data, etc.)
- Clear and measurable objectives that will need to be attained enterprise-wide in terms of efficiency, effectiveness and quality

Transition to a truly consolidated target operating model

Organisations have approached integrated financial crime risk management by assessing the current state for each crime area, enterprise-wide, creating a vision for where they would like to be, developing an outline of the target operating model and developing a roadmap (even if of three years or more) to help get from the current state to the future state.

Assessing the current state for each crime area, enterprise-wide often involves assessing the cost of financial crime risk management, by cost type, considering people, technology and data (including the costs to obtain, store and analyse it), the processes used to manage the data and control its quality, teams organisation and their responsibilities, performance in terms of how it is measured and reported, steps are taken to ensure regulatory compliance.

Creating the future state, often involves looking at the following questions:

- Are we actively seeking out opportunities to align areas of financial crime risk management?
- Who has overall responsibility for managing and fighting financial crime?
- Have we identified areas that can be more effectively aligned, for example, Know Your Customer (KYC) or Know Your Vendor (KYV) data definition (including static and transaction), technology, analytics, investigations, policy and procedures, supporting standards, governance (including functional teams and committees), management information, training development and delivery?

Developing the outline of an integrated target operating model should take into consideration the uniqueness of the organisation and again leverage the findings of the risk assessment.

The key areas of the operating model often address:

- **Strategy:** including financial crime risk definition, identification and assessment, and financial crime policies and frameworks
- **Operations and people:** including structure, skills, process alignment and optimisation, operational effectiveness and efficiency, and talent recruitment, development and training
- **External relations and reporting:** including reporting to the law enforcement authorities, regulatory bodies, industry bodies and contact with the media
- **Governance and compliance:** including compliance with and adherence to policies, assurance testing, periodic policy review, IT system governance, and incident and breach reporting
- **Data and its quality:** including a centralised data hub and data's fitness for purpose, data quality measures and monitoring, root-cause analysis of data quality issues and tools in use

A centralised approach also allows managers to derive key performance indicators, as well as timely and accurate management information, which can be used for essential benchmarking and reporting.

Finally, the exercise should determine how often the effectiveness of the framework should be reviewed and how often the organisation should look for further enhancements.

Developing a roadmap to transition from the current state to the future state will likely involve a set of prioritised initiatives and projects, a high-level implementation plan and a business case, addressing questions such as how ‘effective’ and ‘efficient’ approaches are defined and how ‘quality’ and ‘success’ are defined.

Leverage technology

It is clear that technology plays a critical part in combating financial crime. Technology tools can give an organisation a more holistic view of their data, highlight potential areas of risk and let it be more focused and targeted in its efforts to combat financial crime. While technology is essential, the design, build and execution of this technology must be aligned to the strategy. The technology question should only be answered after the strategy is set: is the technology yielding enterprise-wide results that meet the set efficiency, effectiveness and quality objectives?

Embrace analytics

The target operating model should be constructed around a central analytics hub, the firm's engine room for financial crime risk management, which delivers high quality, actionable insights that can be used to detect, prevent and deter crime. In existing environments, this is often achieved by building a data warehouse that feeds from legacy systems, with a longer-term plan to merge or replace those systems.

Analytics is an underutilised resource for dealing with bribery, money laundering and corruption, according to a new Deloitte survey. Tony DeSantis, principal at Deloitte Transactions and Business Analytics LLP in the data analytics practice, stated that financial crime detection and prevention efforts have often been ad hoc or disparate and not fully integrated in many organisations, and that EFM (enterprise fraud and misuse management) is a way to have a more holistic approach to managing financial crime detection. It can allow organisations to span multiple businesses, and international borders. According to DeSantis, many organisations are unsure of where to begin and how to effectively apply analytics and those out in front are honing early efforts on specific schemes or problematic regions by focused, risk-based approaches and methodologies.

The term ‘analytics’ describes a range of data-driven approaches that, when combined with deep business and sector knowledge, can highlight suspicious activity normally obscured by large data volumes or discrete data channels (data stovepipes). Ideally, the analysis draws on data sources from all over the organisation including operational activity and existing financial crime activity; and potentially from external sources, to establish insights that provide a comprehensive and accurate assessment of risk and is particularly powerful where the criminal activity is dispersed across several data sets.

As links are made between people, account activity and transactions, a wide variety of techniques exist, applied alone or in combination, to reinforce and score links to help analysts make connections and understand the overall risk.

In addition to the data and technology for analysis, the operating model focuses on linking previously disconnected areas of financial crime activity, to explore the overlaps, synergies and linkages that exist between cross-firm data sets. Analysis can focus on historical data, to detect previously unnoticed crimes, or use data flowing into the firm to generate alerts that trigger more in-depth analysis. Ultimately, the data can be used to build models capable of estimating the probability of future crimes occurring, which means firms can become proactive rather than reactive and thereby reduce the potential for significant losses.

As it is based on facts rather than hypotheses and therefore relies both on data volume and data quality, the analytics hub does not try to guess associations. In some cases, data volume can provide a remedy for situations where data has been corrupted either accidentally or through systemic error, or where data fields simply have not been completed.

The use of analytics is often compared to 'finding a needle in a haystack'. The unified approach to financial crime risk management is effective not only because the analytics ultimately finds more 'needles' but also because it very effectively characterises and removes the 'hay', leading to greater efficiency as well as a better understanding of the overall financial crime situation.

Advanced analytics will help companies predict and identify trends and patterns in financial crime risk that are not otherwise easily discernable. Overall, the emphasis must be on prevention and early detection, leveraging technology and analytics to proactively identify issues or potential issues before they turn into front-page news. Analytics based on real-time flows of consolidated enterprise-wide data and not pools of static data will be the key in the future as the data in organisation continues to increase. Analytics, particularly in the context of knowing the key actors (customer, vendor, employee, etc.) must be consistent and holistic across the organisation's businesses and departments. It is not only imperative from a financial crime management perspective but also from an efficiency perspective.

Analytics, particularly in the context of knowing the key actors (customer, vendor, employee, etc.) must be consistent and holistic across the organisation's businesses and departments

Back to basics

Mark Anley, a director at Deloitte South Africa, indicates that the most commonly used prevention mechanisms for mitigating financial crimes are segregation of duties and job rotation, while the most commonly used detection mechanism across the region is quality risk-based internal audits. Perceptive organisations have invested in the development of financial crime programmes that have thorough and detailed enterprise-wide policy requirements, consistent prevention principles embedded in the procedures and controls that have stood the test of time. Such programmes are aligned with the strategy and based on the results of the recurring risk assessment and most importantly contain the key, often basic elements that regulators, consultants and organisations have found to be most effective at preventing and detecting internal and external financial crimes.

These may include:

- External independent testing
- Internal audit testing that is tailored to the risk assessment findings
- Worst-case scenario testing based on actual most famous and/or most recent enforcement actions and media reported cases
- Financial crime type specific training with detailed case studies
- Examples of red flags and end-of-course quiz, testing of system effectiveness by consultants (transaction monitoring systems, sanctions filters, etc.)
- Thorough implementation and recurring testing of the segregation of duties, 'four-eye', 'fit for purpose' and job rotation principles applied to all the high-risk areas identified during the risk assessment

Adopting a proactive approach to testing can assist companies in actively preventing circumventions of their compliance programmes and is usually far more cost-effective than a reactive approach.
Non-compliance with regulatory requirements (both domestic and international) may result in significant financial loss and reputational risk across the jurisdictions in which an organisation operates.

Technology tools can give an organisation a more holistic view of their data, highlight potential areas of risk and let it be more focused and targeted in its efforts to combat financial crime

Change the culture

Failure to prevent or detect issues is often not because the programmes or controls themselves are lacking. More often, it is a failure of culture and a lack of effective change management. For example, senior leaders may not be setting a strong or consistent 'tone at the top' about acceptable and unacceptable behaviours.

This often manifests through fiscal or scope constraints on financial crime projects, dictating an unsustainable bare minimum approach. Alternatively, there simply is not enough attention by all key stakeholders across the entire institution to adopt and execute on the new policies or processes.

Experience tells us that staff training and awareness efforts are often under-resourced. The infrastructure to prevent financial crime may be sound, but its effectiveness still depends on execution, on individuals doing the right thing at the right time—culture is what enables and drives those appropriate behaviours.

Accomplishing this transition typically involves a focused change management effort for the organisation. Executives and directors of financial services companies can no longer support a 'bare minimum' approach to compliance; it is just too risky for the corporation and personally. Corporate collapses and regulatory actions have proven 'bare minimum' approaches have and will certainly fail in the future. Organisations are simply too exposed as they now collect and have access to all the information they require to mitigate financial crime risk proactively.

Executive teams and senior management need to find ways to demonstrate a commitment to financial crime compliance. In addition to setting the appropriate financial crime strategy and communication plan, organisations will often consider making compliance a component of the performance evaluation process to clearly define the compliance responsibilities of management in the different lines of business and departments.

Conclusion

The recent economic crisis has been something of a turning point in the regulatory response to financial crime around the world. An imperative to fight financial crime accompanied by an intense pressure brought about by governments' enforcement actions around the world, has increased the cost of doing business at a time when the private sector was already increasing its focus on risk management. Not surprisingly, the higher level of scrutiny and expectations in relation to financial crime and risk management has become a stay-awake issue for corporate directors and senior management around the world. While it is difficult to quantify the costs of financial crime, there is no doubt that it has become a significant issue for organisations and one that has resulted in significant investments to be compliant with anti-money laundering, anti-bribery and corruption and anti-tax evasion laws and regulations. In a quest to manage their risk exposures more effectively while containing the ballooning cost of compliance, many organisations began to adopt a holistic view to financial crime.

Organisations have successfully transitioned from the pigeonholed approach so loved by agile and flexible 'bad actors' to a consolidated approach to financial crime but not without challenges. In this article, we have provided an account of some key considerations that stem from Deloitte's collective global and cross-functional experience, which include: living by the findings of an enterprise-wide financial crime risk assessment so that it can serve as the starting point for a consolidated financial crime prevention strategy that is resilient. From the latter, transition to a target-operating model of governance, people, process, and controls that is aligned with the strategy and that leverages technology and embraces analytics, without forgetting the basics of effective compliance. Still, failure to prevent or detect issues will result even in the best consolidated financial crime programmes and controls in place if a culture of compliance is lacking. Ultimately, this can only be addressed by senior leaders' setting a strong and consistent 'tone at the top'.