IBM Global Business Services
White paper

Designing for compliance and control

Transforming financial crimes operations through outsourcing, automation, platforms and cognitive

IBM

Throughout global finance and payments, the structural burden of compliance and control in financial crime is forcing new approaches to organizational design. From the Chief Risk Officer (CRO) to the Chief Information Officer (CIO) office, there is an increasing dialogue among financial institutions, governing bodies, regulators, and process and technology operators to reduce detrimental impacts on business value chains, economies, and international security.

Designing for compliance and control targets a reduction in the expanse of effort required to protect markets, organizations, individuals, and security. The aim is to more effectively instill compliance and control throughout the "production process" of financial services, avoiding expensive research, reviews, remediation and rework.

As financial products and services expand at a global scale, the complexities of risk increase. In the last few years, overall compliance headcount has tripled in tier one financial institutions, and compliance costs can now represent 15 to 20 percent of total operating costs with major investments in facilities, technology and skills. Furthermore, the unpredictable nature of associated cost drivers results in significant volatility in cost-to-income ratios and the overall risk profile for the organization.

The activities of financial crime or the use of the financial system for illicit, syndicated activities, such as money laundering, corruption, fraud, cybercrime, terrorism and arms dealing, run into multitrillion-dollar figures. Driven by a maze of data sources and specialized operations, the cost of combating financial crime has increased by over 50 percent in the last three years as seen by many top tier banks.

Banks are not the only institutions that are subject to government legislation surrounding financial crime. Increasingly, any organization that facilitates financial transactions may be in scope for regulation relating to Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT), and Know-Your-Customer (KYC). For example, life insurers, digital payments companies and retailers, all conduct large-scale financial transactions on a daily basis.

Furthermore, governing institutions are increasingly shifting the focus from mere technical compliance toward benchmarking the effectiveness of organizational controls.

Two key challenges in addressing financial crimes are explored: governance and control, and operational inefficiency (with a view toward perspectives on important operational levers now available to financial institutions).

Key challenge 1: Governance and control

Managing large volumes, complexities and fragmentation of multijurisdictional and interlinked regulation creates significant issues in managing financial crimes compliance and the associated legal and reputational risks. Financial flows are really a function of information flows, such as acquiring, exchanging, processing, storing and deciding upon information. The inability to share high-quality information throughout global financial services infrastructure has a series of detrimental impacts on governance and control. In many cases, technology enablement is advancing faster than effective regulatory innovation, and roadmaps for organizational design must be carefully considered against the organizational risk profile and the moving plane of global risk and regulation.

Key challenge 2: Operational inefficiency

The cost drivers associated with financial crime compliance and control are distributed deep and wide throughout the financial institutions. Process inefficiencies are prevalent in interpreting and enforcing rules, scenario planning, reporting and investigative functions. IT and operations inefficiencies, such as duplicative effort, operational rework and legacy infrastructure, all contribute to compliance "bulk." Effective compliance operations are dependent on complex information supply chains involving data standards, large-scale data processing, surveillance, and analytics. Meanwhile, regulatory domain expertise and skilled people to support these functions are an increasingly scarce resource, and resource utilization is a pervasive issue.

Four integrated operating levers

Most financial institutions lack the time and capital to achieve transformational solutions for financial crimes and control. However, important operational levers are available as both componentized and integrated deployments have the capacity to deliver significant returns and improved controls.

1. Outsourcing

While rigorous oversight by the financial institutions is required for compliance outsourcing, a coordinated approach to the lower-risk activities within second lines of defense can yield major benefits. Outsourcing to specialized operators cannot only reduce costs and shift operations toward a variable cost structure; it can also increase capacity, improve controls, and help to better predict cost drivers over time. By transitioning to a standardized, flexible delivery model, the activities of the retained risk and control functions can move toward higher value enterprise services, supporting objectives for growth and keeping pace with regulatory change. The global complexities of information sharing can be managed through coordinated approaches to critical data assets, data quality, lineage, and security. Meanwhile, the pervasive issue of talent management across regulatory, technical and analytical skill sets can be greatly improved with access to talent pools, higher utilization, and embedded metrics for operational excellence.

2. Automation

Robotic process automation (RPA) and cognitive process automation (CPA) technologies are revolutionizing many aspects of knowledge work and changing how organizations view their operations. In financial crimes operations, manual activities associated with multichannel research, data capture and preparation can be automated to free up capacity, while improving speed and accuracy. Robotic controls can be utilized in case management processes, updating of records, and system health checks. Indeed, robotic automation can promote effectiveness measurement for end-to-end alert and investigation processes, automated provisioning and routing of statistics, alert ranking, and stakeholder communications. Compliance and investigation staff can spend over a third of their time in routine, rules-based activities and, most often, welcome the opportunity to engage in higher quality activities and outcomes.

3. Platforms

A platform-based approach to financial crimes enables the pooling of functions and technologies, lowering the costs of ownership and continuous management across infrastructure, software, and hosting. Monitoring criminal activity goes beyond financial transactions, involving numerous semi-structured and unstructured data sources. A platform approach promotes the aggregation and enrichment of large data sets, while high-performance processing and mining engines can perform analytics at a fraction of the cost of relational database processing. Real-time workflows and dynamic monitoring capabilities can be supported through improved interfaces and visualization. Crucially, coordinated platform implementations support improved information security and collaboration, and lay the foundation for driving further economies of scale through innovations in distributed ledger and cloud-based implementations.

4. Cognitive

Cognitive capabilities enable the determination and packaging of insights for efficient scenario planning and decision-making. The ability to process and interpret large data sets has increased dramatically with the onset of machine learning techniques. Organizations can now evolve through supervised to unsupervised machine learning and, thereby, overcome the challenges associated with the availability of historical data for teaching algorithms. Cognitive techniques can be deployed to more accurately tune and model risk, reducing the overload of false alerts generated from outdated systems and processes, and drawing attention to risks previously unidentifiable by other means. Ultimately, the combination of cognitive technologies and network analytics supports real-time predictive and preventative capabilities, enabling more efficient and accurate detection.

In summary, these four levers have the potential to strengthen governance and control for global financial crime activities, with dramatic improvements in operational efficiency.

Furthermore, these operating levers are by no means mutually exclusive, but can be integrated to optimal effect, particularly in industry-specific Business Process-as-a-Service (BPaaS) delivery models. Indeed, outsourced and centralized hubs can provide controlled environments for piloting Regulatory Technology (RegTech) solutions in a cost-effective manner, helping organizations to navigate a sea of innovation in compliance technology. Well-constructed organizational, data and technology architectures can enable the flexibility of an agile framework, implementing short-term accelerators while accommodating for longer-term innovation, complex integration, and new regulation. Skill sets, such as automation management and analytics, can be honed through the application of deep domain knowledge, together with technology and smart, safe approaches to specific risk and regulatory issues.

Governing authorities rely on financial institutions to gain intelligence on financial crime activities, protect individuals, and maintain international security. With more efficient and effective controls, a more accessible financial system can emerge, and with increased opportunities for capital formation and growth.

References

- *Promontory Risk Review, an IBM Company, provides business-process services to financial companies around the globe, transforming clients' risk and compliance operations through our experience, efficiency, and technology. To learn more, visit http://www.promontory.com/PRR/.*
- *Learn about RegTech in the cognitive era: Insights from Gene Ludwig and Bridget van Kralingen*
- *Watch this video and learn more about the importance of trust and reliability in RegTech.*

For more information, please contact:

Ivan Sean Pulley
Global Business Services
FSS, Operations Transformation
1+(917) 239 9624
ivan.sean.pulley@ibm.com
linkedin.com/in/ivansean

Dominique Dubois
Offerings and Methods Leader
Cognitive Process Services
IBM Global Business Services
1 (703) 593-1114
dominique.dubois@ibm.com
linkedin.com/in/dominiquedubois

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
September 2017

GBW03396-USEN-00