Deloitte.

Insight on financial crime: Challenges facing financial institutions

Financial crime has become a stay-awake issue for corporate directors and C-suite executives at banks and other financial institutions around the world. While it's difficult to quantify the costs of financial crime — which can include direct losses, fines for non-compliance, and reputational damage — there is no doubt it has become a significant issue for institutions and one that is more challenging by the day.

For this article, we gathered insights from Deloitte's most-senior financial crime practitioners in the Americas, the Asia-Pacific region and Europe. We asked what financial services leaders should be concerned about in relation to financial crime, and how to manage the issue in today's complex and fast-changing business landscape. Collectively, they identified three broad areas of concern:

	Financial services organizations are struggling to manage and control the many elements of financial crime.
	The threat of financial crime runs the gamut of financial fraud and abuse such as money laundering, bribery and cybercrime. It has therefore become too broad to be handled by established divisions or departments.
	An enterprise-wide approach is essential and should leverage new analytical software tools.

Deloitte's practitioners identified six trends that are driving these broad areas of concern.

Regulation is increasing and becoming more coordinated

Over the past 15 years, financial institutions have grappled with a wide range of new financial crime-related regulation, including measures to address bribery and corruption, tax evasion, financial market abuse, money laundering, terrorism and the enforcement of financial sanctions. Not only must organizations comply with these new conditions, more rules can be expected and regulators are increasingly working in concert globally.

The effect is that regulators are forcing financial institutions to help in policing financial crime. For example, Tracey McDermott of the UK Financial Conduct Authority has said: "Banks and other financial organizations are in the front line regarding protecting against financial crime. We, and they, have a common interest in working in partnership to reduce the impact of financial crime both on the economy and more widely... Financial institutions need to take this responsibility seriously and we will do whatever is necessary to ensure they do."[1]

For several decades, Deloitte has been at the forefront of providing services to help clients — including many of the world's leading financial institutions as well as governments — to deal with the myriad business and compliance issues presented by financial crime.

Deloitte is uniquely positioned to help create and implement financial crime prevention programs. The firm's financial crime network spans across 700 cities in nearly 150 countries and across our main business lines. There are over 10,000 professionals with deep technical knowledge in many aspects of financial crime who regularly draw their deep financial services experience — gleaned from serving 87 percent of the financial services companies listed in the 2013 Fortune Global 500.

Deloitte is ranked #1 in Global Forensics & Dispute Advisory Services, based on revenue, by Kennedy.* In addition, Deloitte has been recognized as a leader by many other leading analyst firms in the capability areas that are critical to providing sound financial crime advisory services. These areas include Forensic & Investigative Services, Dispute Advisory & Analysis Services, Security and Cyber Security Consulting, Business Consulting Services for Governance, Risk & Compliance, Global Risk Management Consulting, and Financial Services Consulting.

*Source: Kennedy Consulting Research & Advisory; Forensics & Dispute Advisory; Kennedy Consulting Research & Advisory

Organizational operational structures are not in sync with the fast-moving financial crime landscape

For the most part, financial institutions have adopted a very reactive approach to a rapidly evolving set of issues, including regulatory developments, economic factors and shifts in the geopolitical landscape. Their main concern is to minimize the financial impact of crime with as lean a structure as possible.

In addition, responsibilities for different types of financial crime often sit in separate divisions, with little coordination or cooperation between the two. This makes responses incomplete and can leave one part of the organization exposed to additional risk even if the immediate problem was handled. More importantly, organizations are not harnessing the value of an effective financial crime strategy, which includes gaining a deeper knowledge of customers and markets, while reducing the potential for suffering damage to their reputations.

[1] "The FCA holds key conference on financial crime," media release, July 1, 2013, www.fca.org.uk/news/the-fca-holds-key-conference-on-financial-crime.

The need for a firm-wide approach to compliance risk management at larger, more complex banking organizations is well demonstrated in areas such as anti-money laundering (AML), privacy, affiliate transactions, conflicts of interest, and fair lending, where legal and regulatory requirements may apply to multiple business lines or legal entities within the banking organization.

There is pressure to adopt enterprise-wide frameworks

National and international regulators are demanding financial institutions pursue more holistic approaches to support those authorities' efforts to increase the stability, integrity and efficiency of the global financial system.

The U.S. Federal Reserve has stated: "The need for a firm-wide approach to compliance risk management at larger, more complex banking organizations is well demonstrated in areas such as anti-money laundering (AML), privacy, affiliate transactions, conflicts of interest, and fair lending, where legal and regulatory requirements may apply to multiple business lines or legal entities within the banking organization."[2]

This new approach involves creating an enterprise-wide framework that can be used to address the full range of financial crimes. This is vital because many organizations have implemented ad hoc tactical responses as regulations have been imposed, often leaving them with an inefficient, inflexible and disconnected patchwork of measures.

Taking an enterprise-wide approach offers the added business benefit of enabling organizations to increase the effectiveness of their prevention initiatives and to streamline their financial crime-related activities.

Breaking down silos and taking a cross-enterprise view of customers and transactions also makes it harder for criminals to exploit gaps between business systems, databases and countries. For instance, the customer intelligence held by banks' credit authorization teams is rarely cross-referenced by AML groups; leaving doors wide open for abuse.

The change management process is not in place to move to a centralized approach

Whether an organization decides to better align and connect existing financial crime prevention offices or seeks to combine them into one central approach, it is likely to be hampered by the lack of an effective change management program. This may include staff and leadership being unaware of the requirements for the program to be effective. To address this, executives should set the appropriate tone at the top and articulate it down the chain of command so there is a common approach. There is also a need for a communications and knowledge framework to support the adoption of those principles by staff.

Cybercrime is the biggest growing threat facing financial institutions and AML remains a central concern

As cybercrime grows in frequency, size and sophistication, it is clear that technological defenses alone are no longer sufficient to protect financial institutions from attacks. Cybercrime has evolved from being vertically integrated and individualistic to an extremely sophisticated and well-organized distributed operation, where stolen data is traded on exchanges by highly specialized professionals.

In addition to neutralizing threats as soon as they occur, an effective incident response is required to understand the nature of an attack, help reduce the cost of data loss, and introduce management rigor and controls that benefit enterprise value.

Money laundering also continues to evolve in terms of complexity and technological sophistication, to the point that even advanced financial institutions are finding it hard to reduce the risk of illicit activity. Because of the pivotal role financial institutions play in the detection and prevention of the laundering of the proceeds of crime, regulators are applying increased pressure on banks to dramatically improve their AML compliance programs. This in turn is creating pressure within the financial institutions community to implement globally consistent controls and processes.

In addition to regulatory pressure, financial institutions face new challenges as new products and services are launched in the marketplace. For example prepaid cards and mobile technologies are rapidly taking the place of cash and other forms of payment, making it easier for consumers to make purchases. These forms of payment can also make it easier for criminals to move illicit funds. As with many innovations — especially within the financial

[2]U.S. Federal Research Supervision and Regulation Letter 08-8. www.federalreserve.gov/boarddocs/srletters/2008/SR0808.htm.

services industry — new risks are a by-product, which will be followed by new regulations.

Financial institutions need to improve their use of technology, including enhancing the quality of the data they hold and updating transaction monitoring, to have truly effective AML programs.

Analytics is becoming essential to effectiveness

With the growth of electronic transactions and the explosion in the amount of information available to organizations, advanced data management and analysis is becoming both the weapon of choice for fighting financial crime and the glue binding enterprise-wide approaches together.

An important factor is that the combination of analytics and big data is allowing financial services organizations to spot potential problems and relationships between parties. This is critical because criminal activity often occurs within networks of related individuals and entities. Advanced data analysis also makes it possible to better predict issues and prevent financial crimes, rather than only addressing them after the event.

For these reasons, the push to resolve financial crime is rapidly becoming a requirement to implement more and more advanced data analytics approaches.

Recommendations for action

The challenge for financial services organizations is to address financial crime by implementing a new approach aligned with these changes. Deloitte believes an effective model is to proactively move towards an enterprise-wide framework, with a strong data analytics capability at the core. However, based on our experience in working with clients worldwide, we are also acutely aware there is a range of obstacles to overcome.

1. Take a holistic approach

The good and bad news for global financial institutions is that no single organization has mastered how to comprehensively manage financial crime. While some organizations have announced large projects and are building dedicated financial crime teams comprising as many as 500 people, even the more advanced are only two or three years into a journey that is likely to last a decade. This means there is still time for organizations to act and keep pace with competitors, but also a lack of clear models to emulate.

In practice, taking a more holistic approach means moving away from federated approaches to more centralized efforts for preventing, investigating and remediating financial crime. Here, the risk management elements that were once handled within silos are linked in an effective, organization-wide program. This involves seeing financial crime as a lifecycle comprising four stages — compliance, prevention and detection, investigation and remediation, and monitoring and testing — then addressing each item.

The financial crime lifecycle

Compliance: Acting in accordance with the requirements of relevant authorities by implementing governance structures and financial crime strategies.

Prevention and detection: Reducing financial crime incidents and identifying early issues and risks by implementing effective operational controls. The focus is on enterprise fraud and misuse management using integrated technology platforms and advanced analytics.

Investigation and remediation: Assessing allegations of fraud or financial mismanagement, responding to government regulatory requests, and helping financial services organizations remedy issues and prevent their reoccurrence. This involves data assessment, e-discovery, understanding relevant laws and regulations, and undertaking cyber response activities.

Monitoring and testing: Assessing financial crime systems and policies to ensure they are efficient and tailoring systems to meet changing internal and external threats.

In tandem, the organization should assess its current state, set a vision for the future state, develop a roadmap for getting there, and outline a target operating model. During this process, the organization should search for synergies between its financial crime intelligence and customer intelligence initiatives to identify opportunities for improving customer service and adding value to the business. The more this can be achieved, the greater the economies of scale and the better the chances of cross-domain bearing fruit.

2. Be prepared for significant cultural change

Institutions shouldn't underestimate the cultural and operational change program required to take a more holistic approach to financial crime. This should begin with setting the tone at the top of the organization and continue by working diligently toward buy-in from stakeholders, having a clear and effective communications program, and allowing sufficient resources for training staff and managing workforce transitions.

A common issue for organizations will be that the various

aspects of financial crime — such as fraud, money laundering and cybercrime — are handled by separate teams. Not only do these groups focus on discrete parts of the puzzle, they also hold different perspectives.

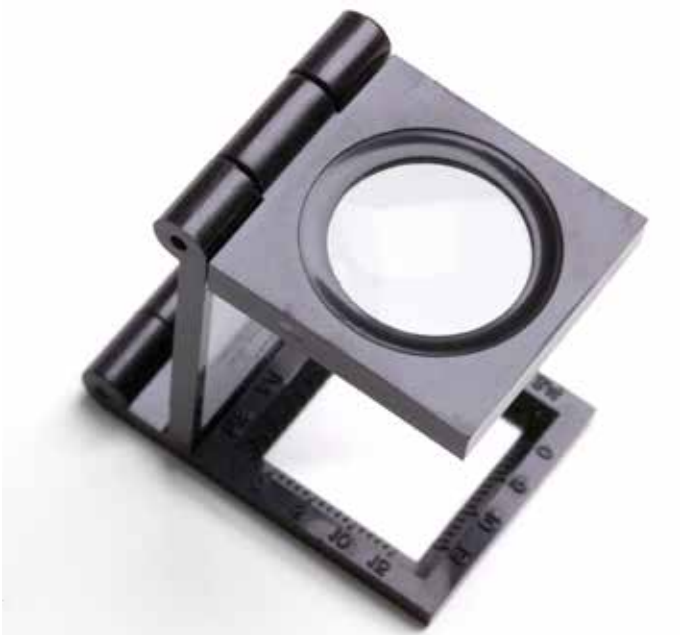
The biggest split is typically between anti-fraud groups charged with eliminating problems that cause clear and direct losses to their firms, and other groups focusing on issues such as money laundering and tax evasion, which are illegal but not regularly of immediate concern. There can also be large variations in risk tolerance and willingness to absorb losses as part of doing business.

Taking a genuinely enterprise-wide approach to financial crime therefore requires significant levels of internal communication and agreement, and can result in significant changes. For example, Deloitte has seen institutions relinquish up to 30 percent of their customers as part of programs aimed at making their organizations compliant and resilient.

3. Improve the quality of your data

The larger and more distributed a financial organization becomes, the harder it is for it to access consistent, high-quality and standardized data. This is particularly true for institutions that have multiple technology systems because they have grown through acquisition, and those that have offices in countries such as Switzerland with restrictive data transfer laws.

In response, organizations should focus on improving and standardizing data to increase their capacity to perform centralized analysis. They should also explore the use of the latest analytics techniques, which make it possible to still derive insights from unstructured information sources or data from disparate systems across the enterprise. The more sophisticated systems can not only help predict problems, they can learn as they go.



4. Secure the right talent — centrally and locally

The battle to solve financial crime is rapidly evolving into a race for the talent required to mount an effective defense. Our clients are experiencing a particular shortage of individuals capable of completing more analytical and critical assessments in emerging market locations, including parts of Africa, Asia, and Central and South America. They are also finding it desireable to have strong capabilities "on the ground" close to customers, especially in locations that may be very different to the countries in which their central corporate governance and compliance teams are located.

5. Prepare for the future

Finally, a new framework for addressing financial crime should consider both current and future threats. As with the rise of online banking in recent years, crypto-currencies are opening up new avenues for criminals. We are also seeing a rapid evolution in payment technologies; issues regarding commercial espionage; and a growing interest in how financial institutions can help authorities monitor money flows into and out of burgeoning sovereign wealth funds. To accommodate these trends, new frameworks should be built to expect the unexpected and allow for relatively rapid change.

The silver lining

The ongoing expansion of financial crime in the age of the Internet and regulators' efforts to address it couldn't come at a worse time for many large financial organizations. Many banks in particular are already strapped for resources at a time when they are urgently seeking to re-establish their financial stability, foster ethical cultures and rebuild profitability after the global financial crisis and other recent scandals and turmoil.

However, Deloitte is confident that taking an enterprise-wide, analytics-driven approach to addressing financial crime is not only achievable but can provide potential cost and performance gains well beyond the compliance function. These potential gains include streamlining and increasing the effectiveness of current compliance measures, and developing systems that improve customer service and marketing effectiveness. Such an approach will also give institutions the performance indicators needed for vital cultural change.

Contact us

APAC Financial Crime Leadership Team

Deloitte Singapore

Tim Phillipps
Global Leader, Forensic & Analytics
Singapore and Southeast Asia
+65 6531 5034
tphillipps@deloitte.com

Victor Keong
Executive Director, Enterprise Risk Services
Singapore
+65 6224 8288
vkeong@deloitte.com

Matt Bailey
Executive Director, Consulting
Singapore
+65 6232 7124
mattbailey@deloitte.com

Wilds Ross
Executive Director, Analytics
Singapore and Southeast Asia
+65 6531 5079
wildsross@deloitte.com

Deloitte Australia

Ivan Zasarsky
Partner, Enterprise Risk Services
Australia
+61 3 9671 7252
ivanzasarsky@deloitte.com.au

Deloitte Hong Kong

Nick Robinson
Partner, Asia Pacific Forensic Leader
Hong Kong
+852 2238 7085
nickrobinson@deloitte.com.hk

Deloitte Indonesia

Widiana Winawati
Partner, Forensic
Indonesia
+62 21 2992 3100 Ext. 30980
wwidiana@deloitte.com