NICE · ACTIMIZE

Understanding & Managing Financial Crime Risk

White Paper

TABLE OF CONTENTS

NICE · ACTIMIZE

What is Financial Crime Risk?

Of the many vulnerabilities and threats to the financial services sector, financial crime risk has emerged as a pervasive, yet widely misunderstood category of risk. As consumers, governments, and the financial industry have gained familiarity with various forms of financial crime, financial services organizations have seen that the underlying risk of financial crimes not only includes the direct action taken by criminals, but also includes the impact of deterrence, detection, and resolution on the organization and its customers.

But what is financial crime risk? As the term is only now becoming part of the lexicon of the financial services sector, establishing a single definition will help guide the discussion and eliminate misunderstanding:

A financial crime is a ***regulatory, reputational, or monetary act or attempt*** against financial services institutions, corporations, governments, or individuals by internal or external agents to steal, defraud, manipulate, or circumvent established rules.

The essential aspect of this definition is the impact beyond the actual financial criminal act itself, because financial institutions feel the effect of these incidents far beyond the specific incident or situation. Working with this definition, there are three main areas of financial crime risk posed to financial services organizations:

- Criminal Acts: These include actual financial crimes and explicitly illegal acts, such as account takeover, insider trading, illicit employee activity, terrorist financing, and market manipulation. Most financial institutions and consumers are able to identify these types of activities and their downstream effect.
- Compliance & Monitoring: Activities such as trading and sanctions compliance, suspicious activity monitoring, and Know Your Customer (KYC) requirements are typically driven by regulations and are traditionally seen as just the cost of doing business. More recently, financial services organizations have come to understand how technology and processes affect investigators, compliance officers, and customers. Continued investment in intelligently combining technology with processes is now often mandated in an effort to limit regulatory fines, sanctions violations, and other financial crime risks. This also helps financial services organizations to gain additional value from compliance programs, either through greater efficiencies or by leveraging collected data in sales and marketing activities.
- Intangible Impacts: These “softer” effects include the indirect impact of prevention, the burden placed on internal processes, as well as the possible negative impact of customer disruption and reputational damage. Additional examples of less tangible impact include finding extra resources to support timely regulatory filings or examinations, increased data storage needs, and the “cost” of enforcing audit and supervisory procedures such as ongoing education and the opportunity cost of neglecting “regular” activities. Often, these opportunity costs are not calculated in the total cost incurred to an institution despite their significance.

NICE · ACTIMIZE

Dealing with a Growing and Public Problem

With financial crime, any news is bad news, and there has been no shortage of bad news lately. Whether the topic is the loss of monetary or informational assets, regulatory scrutiny, or costly reputational damage, the issue of financial crime and the wider effects on the financial industry are in the headlines now more than ever before. But while the effects of financial crime are apparent, efforts to prevent it are not as easily executed.

Financial services organizations have the difficult task of effectively identifying the greatest risks to themselves and to their customers, protecting both parties against unnecessary risks and satisfying regulatory requirements for greater transparency, awareness, and consolidation of information across the organization. For many such organizations, this challenge is compounded by a stagnant or even shrinking budget allocation, making these tasks even more daunting. Financial services organizations are increasingly realizing that they must move beyond the traditional reactive and siloe'd approach toward a more comprehensive Financial Crime Risk Management strategy.

Understanding Financial Crime to Manage Financial Crime Risk

The myriad challenges encompassing financial crime risk require a change in institutional mindset and a greater understanding of what to look for, how these incidents occur, and what means institutions have to resolve and remediate them. The initial step in building this awareness of financial crime risk is in understanding how different types of risk manifest themselves beyond functional or divisional segmentation. When viewed from a high level, effectively managing financial crime risk falls into three main categories:

Prevention Risk

The initial phase in the lifecycle of financial crime risk deals with threats that have not yet affected the institution; this can be thought of as the programs and activities to halt any suspicious or non-compliant activities before they become an issue. For financial services organizations, many of these activities require a great deal of resources and insight into customers that may not be available or easy to aggregate.

These examples highlight the complexity of prevention and associated risks:

- Stopping suspicious persons from opening accounts or moving funds into the institution prevents risk to the institution, but may also turn away legitimate customers, thereby decreasing new business.
- Balancing the risk of doing business with suspicious entities without completely closing off from high-risk regions in which valuable customers and businesses reside or do business.
- Deterring illicit actions from internal and external parties diminishes threats, but may cause unwieldy and frustrating controls, thereby inadvertently upsetting customers, partners, or employees.
- Ensuring the network isn't being used with infected devices requires constant vigilance, dedicated resources, and an understanding of the ever-shifting digital threat landscape.
- Determining the suitability of new clients and their own risk appetite according to the appropriate regulations requires ongoing training and education of personnel.
- Identifying potential risk areas and challenges having to do with client relationships, accounts, information, and transactions before a problem occurs is both extremely valuable and extremely difficult with information silos across complex institutions.

The challenge of preventing financial crime risk is extremely difficult, perhaps more difficult than that the other phases of the financial crime risk lifecycle. It requires a delicate balance between legitimate activity and risky activity, often with little or no transactional or behavioral background (i.e. in the case of opening a new account). In addition, the time required to make these decisions is typically quite short, with a yes or no decision oftentimes meaning the difference between a customer relationship for the next decade and giving business to a competitor.

However difficult it may be to do, identifying not just active, but also potential threats, enables financial services organizations to diminish risk and reduce the costs associated with losses, fines, investigations, and customer remediation. Proactively addressing financial crime risks requires a great deal of collaboration and coordination across the institution, but provides tremendous benefits to the institution and reduces both risk and cost.

NICE · ACTIMIZE

Detection Risk

The next phase in the financial crime risk lifecycle involves identifying and responding to threats that are active or ongoing. Effectively handling these types of risks requires both accuracy and speed, as a few seconds mean the difference between stopping a criminal act or suffering the effects of a financial or data loss, compliance violation, or major customer disruption.

Financial services organizations have acquired and built a myriad of systems and sensors to monitor for specific events and types of behavior; however, the many technologies lack the wider scope needed to see incidents in context. That lack of greater visibility often allows complex, cross-channel schemes to go undetected as criminals exploit the gaps between detection systems.

The challenge of detecting complex risks within financial services organization includes:

- Identifying deviations and anomalies or unexpected changes for a single user across all the devices, channels, and activities with which they interact with the institution.
- Monitoring such changes and anomalies in customer behavior, account usage, suspicious patterns, behavior, financial or non-financial transactions, and seeing the interconnectivity between activities as well as how certain sequences increase risk.
- Comparing how user behavior shifts over time as compared to prior behavior, prior account usage, peer groups within that individual account or organization in a way that is fast enough to react to events, but scalable across all of the institution's customers.

Detecting a suspicious incident among millions or even billions of transactions and non-monetary activities requires broad coverage against various avenues of risk as well as the intelligence to correlate patterns from across the organization into a single, context-driven decision mechanism. While financial services organizations often have greater context when detecting risk than when preventing risk, the challenge is no less difficult as patterns continuously shift. This means that the detection methodology and technology that is effective today may not be as useful in the near future.

Maintaining effective financial crime risk detection is an ongoing activity. Financial services organizations have found success by developing programs that both learn continuously from customer activity and preserve more traditional model and precedent-based detection logic, all the while adapting to new patterns of risk. By constantly looking at these patterns and understanding the nature of threats and vulnerabilities, institutions can separate anomalous, but low-risk activity from truly suspicious acts. This has the additional benefit of not overloading staff with alerts and not unnecessarily disrupting customer experience.

Investigation Risk

The last phase of financial crime risk is often the most overlooked, but it underpins the entire financial crime risk lifecycle. While prevention and detection each deal with types of risks, investigation encompasses how those risks are handled and resolved once they have been identified. Intuitively, the necessity of this step in the overall lifecycle makes sense; however, the often unnoticed aspect is how essential the manner in which issues are discovered and decisioned affects the institution in terms of both risk and cost.

Highlighting how different effective resolution and investigation of risks can be from traditional, often human-driven analysis shows how great of an impact this step has on an institution. Done properly, this means a financial services organization is:

- Ensuring analysts address the highest risk incidents first, reacting quickly before major issues or losses occur as opposed to handling events in the order they occurred.
- Keeping managers and supervisors aware of what's happening as it happens, in terms of emerging risks and analyst productivity, rather than waiting until a periodic reporting time when it is too late.
- Creating processes and workflows so that analysts treat each incident the same way and resolve issues in a predictable amount of time.
- Automatically recording all analyst activity for future audits and capacity planning, instead of relying on investigators with varying levels of experience to identify complex threats across multiple point solutions.
- Streamlining actions performed by solutions, thereby speeding issue resolution and lowering overall costs.

An organization's reaction to an event is just as important as awareness of the incident in the first place as demonstrated in the examples above. Proper prioritization of risks and correlation of activity across departments, jurisdictions, and functional areas requires capabilities beyond that of even the best-trained investigator. Developing processes and technology that not only automate low-risk activities, but that also provide insight to human investigators on complex, suspicious incidents is a true "game-changer" in Financial Crime Risk Management; moreover, it has the potential to save the organization significant operational costs while also eliminating the artificial barriers between information silos.

NICE · ACTIMIZE

Strategic Approach to Financial Crime Risk Management

The challenges to financial services organizations are numerous; however, with the knowledge of the various stages of both Financial Crime Risk and Financial Crime Risk Management, the ability to strategize and develop skills, processes, and systems that mitigate these risks becomes more feasible. Such programs are most effective when implemented comprehensively, involving areas of the organization that are affected by all three phases of the financial crime risk lifecycle. These programs should also stress the best practices from effective Financial Crime Risk Management at similar firms takes and leverage those strategies for organization-wide risk coverage.

5 Pillars of Financial Crime Risk Management

In recent years, the concept of a consolidated and intelligent Financial Crime Risk Management program has been gaining traction among financial institutions both large and small. The common thread among such organizations is the vision that the program should not only mitigate the risk of threats to the organization and to its customers, but that it should also provide additional benefits such as operational efficiency and improved customer experience.

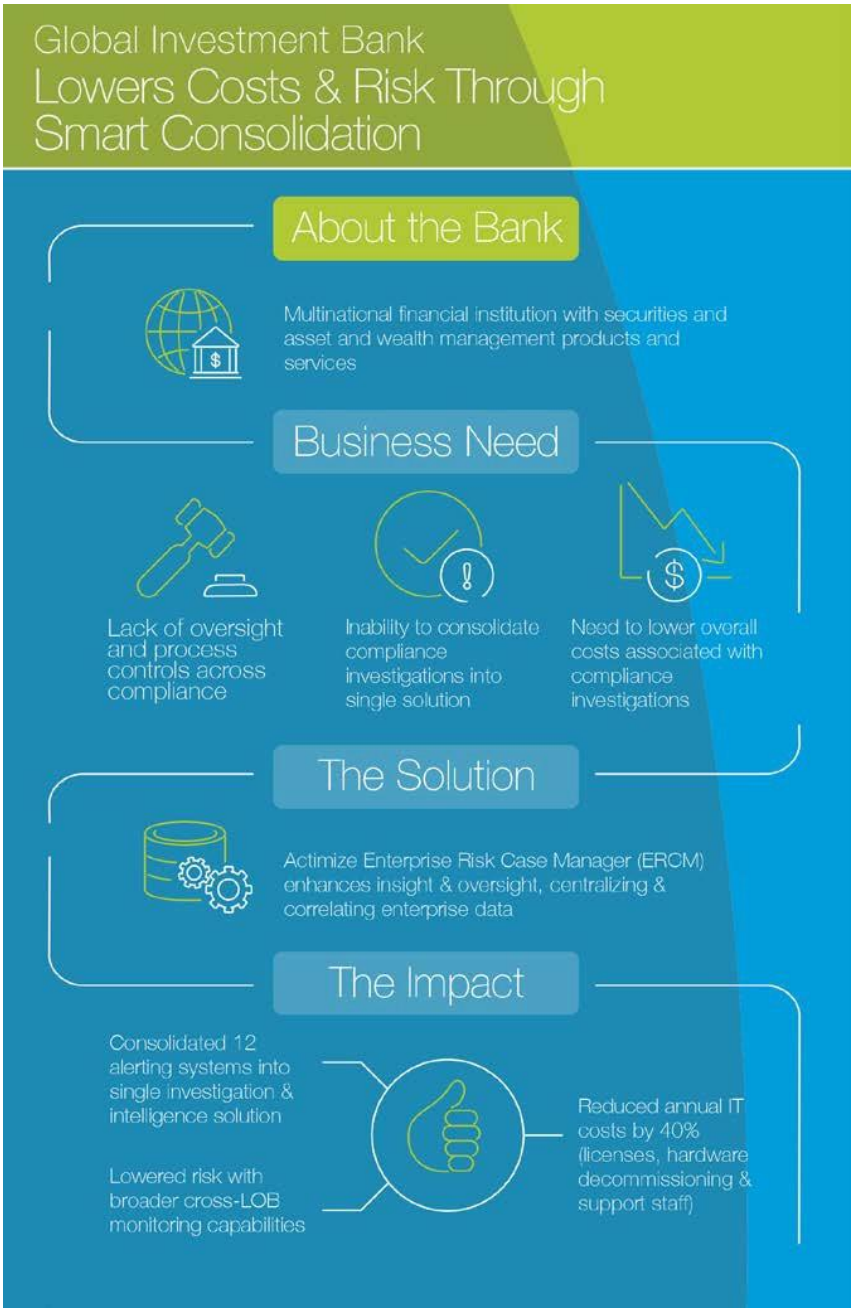
Financial services organizations should look beyond end-point solutions and investment in individual functional areas and instead build an effective and comprehensive Financial Crime Risk Management program that espouses the following characteristics:

1. **Holistic:** Gaining transparency and a greater view of risk by connecting data and systems across disparate groups, channels, and silos is essential to identifying potential risks and ongoing threats to the institution. Shrinking such gaps directly translates into reduced risk to your organization and customers and in time will deter criminals looking for easy targets.
2. **End-To-End:** Preventing, detecting, and investigating incidents before they affect your business and your customers is as important as initially identifying the threat. But the process should not end at resolution alone; learning from incidents as they are resolved enables your organization to iteratively improve all elements of the financial crime risk lifecycle by including speedier resolution and detection of similar incidents in the future.
3. **Customer-Centric:** Increasing the accuracy of detection, lowering the number of false positives, and reducing unnecessary disruptions to customer activity are all crucial to ensuring customer satisfaction and to creating a more effective prevention program. With increased context of an individual customer, the financial services organization can fine-tune profiles and continuously improve results, eliminating wasted time for analysts and investigators.
4. **Automated:** Lessening the amount of human capital and infrastructure needed to maintain effective risk and compliance controls is a top priority. Automation enables organizations to focus human investigators on the areas that need them most and to thereby leave manual and mundane tasks to systems that perform them in a fraction of the time that a human being would. Beyond prioritization, using technology to pull together related information and incidents increases the time an institution has to react to a given event.
5. **Adaptive:** Ensuring agility and responsiveness as risks, regulations, and business needs change and evolve over time is a necessity for today's ever-evolving regulatory and threat environment. The ability to grow and adapt provides financial services organizations with greater coverage against risks and the ability to enter markets quicker and more confidently to keep pace with the competition.

Much like any complex issue, there is no one single action or activity that eliminates the problem. These pillars provide the basic framework for a financial crime risk program that ensures compliance and coverage against threats while also ensuring the necessary resilience to adapt to changes in the market. These pillars also provide financial services organizations with the means to achieve some of their top goals: improving customer experience, lowering ongoing operational costs, and mitigating risk to the organization as a whole.

How Firms Deal With Financial Crime

Some financial institutions have already had success building and executing on this Financial Crime Risk Management strategy with an eye on the big picture. Below are some of the ways this has been achieved, along with the resulting business benefits.



NICE · ACTIMIZE

How NICE Actimize Helps Financial Services Organizations Manage Financial Crime Risk

NICE Actimize has worked with hundreds of financial institutions around the world on all areas of Financial Crime Risk Management. With proven technology and a wealth of subject matter expertise, NICE Actimize helps these institutions identify, plan, and execute on a consolidated financial crime approach that focuses on:

- Consistent processes
- Compliance with regulations & regulatory expectations
- Lower cost & lower total cost of ownership
- Better coverage with fewer gaps

As risks to financial services organizations and their customers grow and change, a consolidated, comprehensive approach to Financial Crime Risk Management will provide the greater risk and compliance coverage needed to keep pace with an ever-changing marketplace. Financial Crime Risk Management also accomplishes this while also achieving the efficiency and cost effectiveness that demonstrate tangible return on investment. It is this balanced approach - acknowledging the need for both efficacy and value - that supports a long-term financial crime strategy, continuously validating the business case for ongoing investment.

Ultimately, financial services organizations gain additional value from their Financial Crime Risk Management programs, but doing so with a long-term approach is crucial. By building toward a unified, consolidated program with each technology investment and integrated process, financial services organizations create the foundation of a Financial Crime Risk Management program without the need for massive shifts in technology, processes, or training of personnel.

ABOUT NICE ACTIMIZE

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

info@niceactimize.com | www.niceactimize.com | www.niceactimize.com/blog | @nice_actimize | linkedin.com/company/actimize

NICE · ACTIMIZE