PROTECT **THE BANK**

CGI

Experience the commitment®

Introduction

This white paper discusses what regulated bodies should be concerned about in relation to financial crime. It describes a new holistic approach for addressing financial crime in today's complex and fast-changing regulatory landscape and how that approach can deliver huge benefits, including significant cost reductions while, more importantly, raising the level of protection for the institution.

With the current regulatory landscape impacting different business areas, such as anti-money laundering prevention, anti-fraud management and cybersecurity, identifying exactly which regulation impacts which business area is practically impossible. This multi-dimensional complexity impacts people, processes and technology in such a way that the current silo-based approach used by most major financial institutions is no longer sufficient.

In this paper, we will introduce a new comprehensive approach that unifies the silos into a unique integrated financial crime architecture. This approach involves cybersecurity, big data, intelligent self-learning, and case management processes and technologies, all working together to drive efficiencies and performance in combatting financial crime.

The current situation

Compliance and risk management professionals in the financial services industry are struggling to provide the multiple dimensions of control required to handle the varying aspects of cybersecurity and financial crime. While disparate regulators around the world have made the compliance landscape hugely complex, criminals continue to focus on staying one step ahead of the tools and processes used to prevent them from succeeding.

The threat of financial crime now includes financial fraud, money laundering and bribery, as well as a raft of new cybercrimes, which can be even more difficult to monitor and prevent. The threat has become so diversified that it is impossible for individual units or departments operating in silos to effectively manage it.

The globalization of finance and the development of instantaneous electronic payment systems across multiple devices have had an unparalleled impact on the evolution of fraud. By the end of 2017, many countries will process transactions in real time (using a block chain, permission-less distributed database protocol), so delinquent patterns will need to be detected within nanoseconds. This also presents considerable challenges for the monitoring of transactions, sanctions screening and customer due diligence.

The increasing threat

Across the globe, countries are moving to instant payments, building new infrastructures that enable consumers to move money in real time from one account to another. In Europe, the new SEPA instant payment infrastructure will come into operation in 2017. Once fully operational, this will enable consumers to send funds across borders in real time, creating another new business area that will need to be monitored. As these new schemes begin to communicate with one another, new areas of the bank will need to be monitored and require additional fraud checks. At the same time, transaction volumes within traditional compliance areas continue to grow.

Both of these factors mean that more business areas and more transactions will need to be scanned and monitored. As more transactions are scanned, more alerts will be produced and, therefore, more manual work will be required for rejecting or accepting the transactions.

In addition, a sophisticated and self-sufficient digital underground economy in which data is the illicit commodity is growing. Stolen personal and financial data has monetary value because it can be sold or used to gain access to existing bank accounts and credit cards or to fraudulently establish new lines of credit. This drives a whole range of criminal activities, such as phishing, pharming, malware distribution and corporate database hacking. And, this web of crime is supported by a competent infrastructure of malicious code writers, as well as individuals able to lease networks made up of thousands of compromised computers to carry out automated attacks.

Due to new technologies, advanced, multi-dimensional cybercrimes have reached a level of sophistication that renders conventional law enforcement methods ineffective. Mitigating and responding to these new types of crimes will continue to be a problem, as predicting threats and new patterns is very challenging. The unprecedented scale of the problem threatens the ability of authorities to respond with, according to one estimate, more than 150,000 viruses and other types of malicious code in global circulation and more than 148,000 computers compromised per day.

On the other hand, authorities have more criminal activity data at their disposal than ever before, which greatly improves intelligence gathering and enables them to complete investigations in a more streamlined and cost-effective way, given the right tools and processes.

A time of transformation: Customers in a digital world

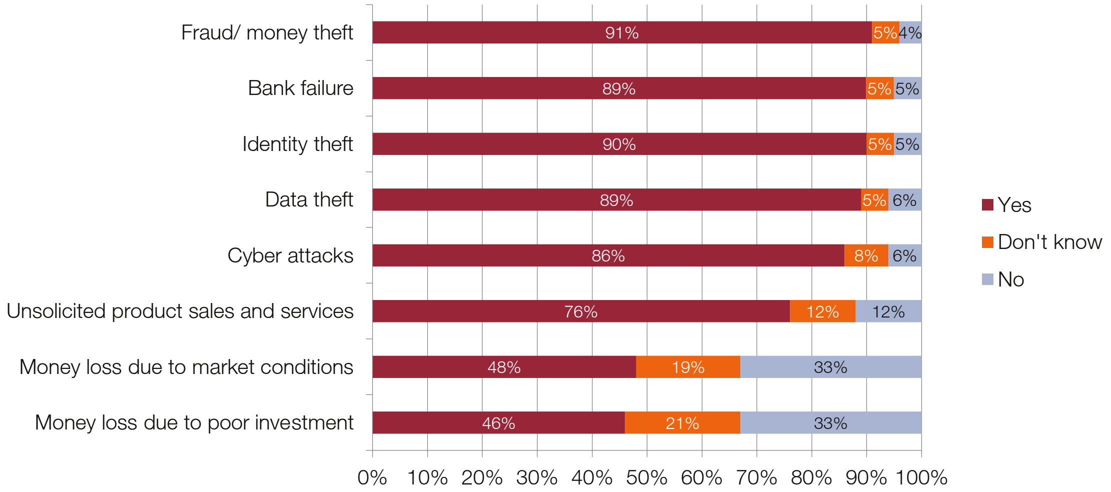
Customers now demand anytime anywhere banking. This requires innovation and robust security optimized to meet the expectations of technology-oriented customers.

Digital transformation is much more than just a change from traditional to digital banking. To preserve customer loyalty, it is vital for banks to learn and understand their customers' behaviors and preferences. The focus is not only on products but also on people.

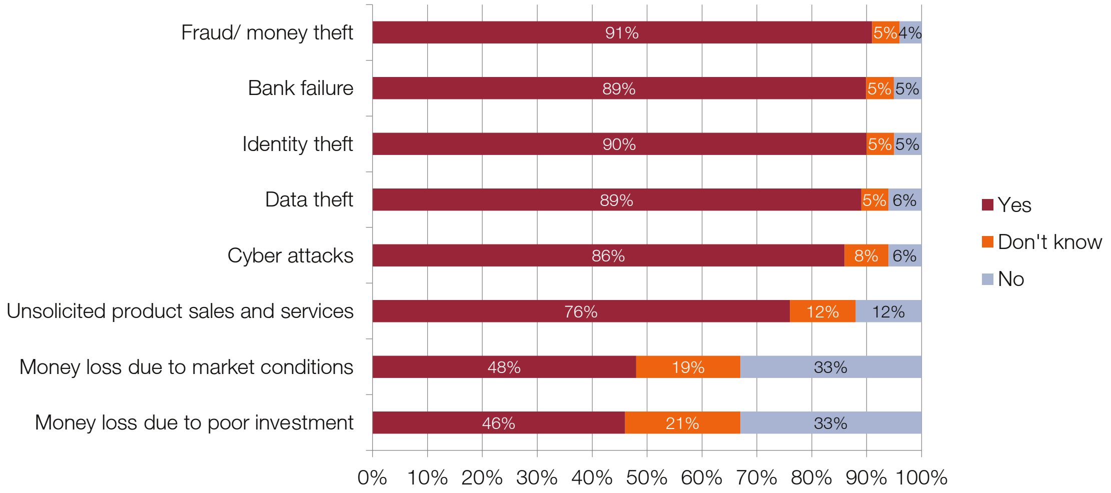
Consumers make their choices very carefully and, according to a recent CGI survey, Financial Consumer Demands for Tomorrow's Digital Bank, they take protection against cybercrime and fraudulent activities very seriously. Most expect their banks to implement the highest possible measures to combat financial crime, which is a good example of how compliance can generate gains for business.

Bank consumer security preferences

My bank should protect me from…



My bank does protect me from…



By implementing best security practices and then promoting that implementation across traditional and social media channels, client loyalty can be increased and market perception improved.

Consumers are willing to leave their bank if their needs are not met and, inversely, if the bank meets their expectations, business will increase. Summarily, this means that understanding consumers in the digital era is key. The focus must be on the customer.

When compliance goes wrong

Our recent research clearly demonstrates that financial institutions spend a huge percentage of their run budgets on compliance. In fact, in many cases, the cost of compliance is so high now that it is impacting their ability to deliver strategic projects, such as digital transformation. Banks that do not transform are beginning to be undermined by the new FinTech start-ups and challenger banks.

Many financial institutions find themselves stuck in a vicious circle. Funding is unavailable, and, therefore, they cannot transform fast enough, so the problem just gets bigger.

Clearly, with fines from regulators continuing to grow at alarming rates, together with the reputation damage caused by getting it wrong, noncompliance is not an option either.

Interestingly, many of the fines levied by the OFAC in recent years have resulted from inside threats, where a criminal has managed to get inside the bank and modify transactions or data, so that records bypass the normal controls. So, even when best practices are in place and underpinned by solid transaction monitoring, it can still go wrong.

There must be a better way

The current situation of banks and other businesses requires multi-dimensional, efficient and effective financial crime management. The regulatory landscape has grown so complex that fraudsters can now bypass and evade controls and, at the same time, the cost pressure is immense. Moreover, combatting financial crime goes hand in hand with interdisciplinary knowledge. A single-dimensional view is no longer sufficient. Financial crime prevention now cuts across all corporate structures, processes, and products and can involve multiple parties.

These challenges can be managed only with a strong and integrated financial crime platform and a deep understanding of the other aspects mentioned above. Information technology, data and financial crime operational know-how go hand in hand.

An omni-channel strategy can bring together all of the key parameters—online and offline channels, data and technology, customer behavior and experience—onto a single platform. Although the concept of a single platform has been around for quite some time, banks and businesses have shied away from adoption, mainly due to critical considerations related to the required applications, technology support and operational changes, as well as issues such as operational silos, online services that need to be monitored in real time, and conflicting priorities.

If successfully implemented, a strong holistic approach can lead to improved brand recognition and revenue, more customers, an enhanced customer experience and stronger competitive differentiation.

Let’s look at the components needed in a modern holistic approach to fighting financial crime.

First, the bank needs to ensure that it has a state-of-the-art sanctions screening solution, strong fraud detection capabilities and know your customer processing. Currently, these are often installed and working but within their own silos. To create an effective next generation solution, the silos need to be broken down and the components integrated both to enable better performance and to ensure greater control and reliability.

Centrally controlling alerts – Case management

Case management is a critical tool for combatting financial crime in an environment of enhanced regulatory scrutiny and increasing costs.

Achieving tighter internal controls to improve anti-money laundering, fraud prevention and sanctions compliance while reducing costs is becoming increasingly difficult given the high volume of exceptions, the constant stream of complex new regulations, disconnected suspicious activity monitoring and fraud detection systems, and cumbersome manual processes.

Strong, centralized technology – Command and control center

It is becoming clear that the borders between siloed bank operations are increasingly overlapping and, with the world moving to real-time processing, now is the time to break these silos down and take a holistic approach to fighting financial crime. Cybersecurity breaches in many ways are equivalent to financial crime breaches, so to minimize costs and reputational damage, the implementation of strong technological controls is a key factor in combatting crime and providing good audit trails.

As the silos are broken down, the individual business areas can send all alerts to a single integrated case manager, which combines and manages all hits and notifications. Effectively, it becomes the command and control center for effective management of alerts, sanctions, fraud, suspicious activity and cybercrime.

Continuous learning and improvement – Intelligent self-learning

Due to the underlying complexities of the data, it is important to implement a single intelligent self-learning (ISL) suite that can provide efficiency improvements across the business areas. It is not just about the fraud itself; erroneous charges and fines levied by credit card processors on customers are secondary consequences of fraud that can have a major impact on a business' bottom line. A thorough understanding of customer behavior resulting from a system applying ISL can effectively analyze a situation and enable the business to take steps to end the fraudulent behavior, or at least prevent it from happening again.

ISL is one of the most important requirements for any financial crime platform. Software that has a self-learning capability generates a feedback loop that improves filters by automatically discovering the good guys, thereby reducing the number of false positives and streamlining the review process. A self-learning capability has been shown to reduce the number of false positives by up to 70%, without reducing the filtering accuracy or narrowing the net.

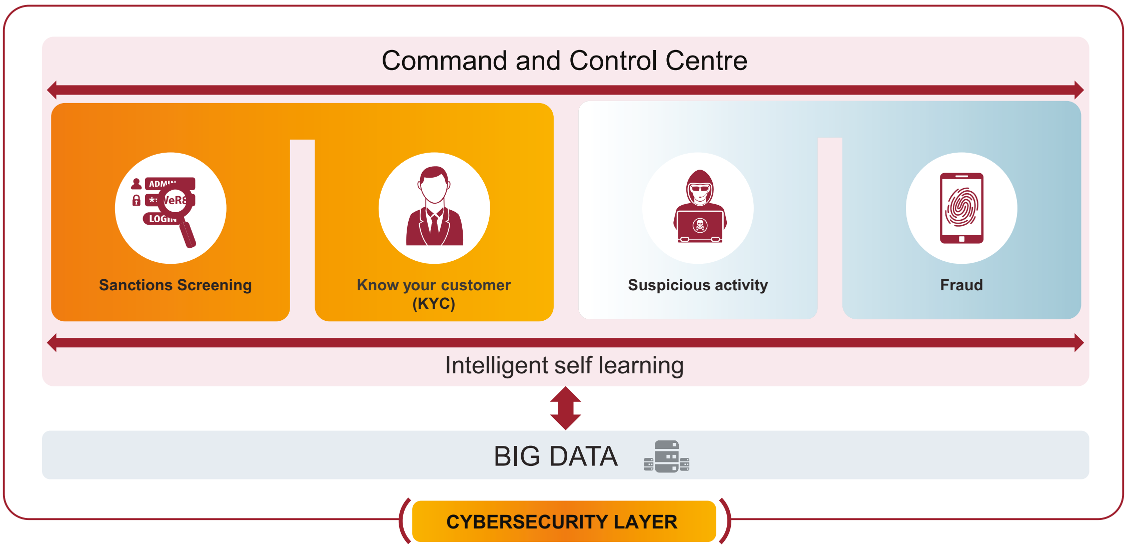
As fraud patterns are identified, so are the levels of risk attached to certain countries, behaviors, types of customers, etc. The attachment of a risk to a factor is the start of an automated risk management solution and the development of best practices that protect businesses from fraudulent transactions while preserving operational efficiency.

Big data analytics and big data management

In many cases, data (whether big or small) is somewhat unstructured, e.g., payment instructions, handwritten notes, disparate electronic lists, etc., which can help facilitate financial crime. Alongside screening tools that can read and process unstructured data, having the ability to structure the data into a streamlined digital process is vital to managing the problem. A key element of this structuring is an integrated IT portfolio, designed with the business's regulatory requirements in mind. This can serve as a single repository for all data and have a positive impact on the quality of the data in terms of consistency, completeness and timeliness of presentation.

Many institutions already use ISL type solutions within their silos, for example to improve sanctions screening. However if the solution is extended across all areas, and provided access to big data sources, then new algorithms could be implemented to drive significant efficiency gains across the different business areas and processes improving effectiveness and overall protection. This would involve the sharing of knowledge so that fraud systems and sanctions systems would effectively begin to talk to one another, sharing knowledge and results in real time.

CGI'S Protect the Bank Architecture



CGI's Protect the Bank architecture integrates the four distinct pillars required for effective financial crime management: sanctions screening, know your customer, suspicious activity monitoring and fraud prevention.

However, the new architecture brings these together under a single command and control center, or case manager, where all alerts and notifications can be centrally distributed, processed and monitored.

To drive the efficiency gains required, each component utilizes the intelligent self-learning which operates across traditional silos and off big data sources.

Let's now look at some of the core components and processes of Protect the Bank in more detail.

Sanctions screening

Organizations must have a robust filtering software solution that meets today's demands from both an operational and technical view.

Regulated organizations face considerable challenges as they strive to comply with ever-expanding legal requirements for combating money laundering and terrorist financing. From an operational point of view, sanctions screening addresses the growing number of global watch lists and sanctioned activities as organizations are pressured to extend their screening processes across the entire enterprise.

Real time sanctions screening and screening for politically exposed persons (PEPs) create additional layers of complexity. Watch list data can change daily, further complicating the task of maintaining an up-to-date, efficient screening operation. Each new watch list requirement increases the compliance burden, while potentially slowing transactions and customer service.

Financial institutions now more than ever are caught between their obligation to prevent illegal transactions and the rising costs of compliance.

Having world class screening controls in place is more important than ever. Individual corporate executives have been prosecuted and jailed, and banks have been fined hundreds of millions—even billions—of dollars for alleged dealings with blacklisted nations and drug cartels, and for deliberately or inadvertently helping them launder money and evade sanctions. As the global fight against money laundering and terrorist funding expands, the obligation to monitor transactions is expanding beyond financial institutions to affect large corporations, insurance companies, money transfer services and other types of businesses.

Robust sanctions screening can significantly reduce the time and cost required for sanctions compliance by analyzing all transactions and automatically alerting companies to potential matches against watch lists. The most effective software limits the number of "false positives" that mistakenly flag legitimate transactions as suspicious, without letting any sanctioned transactions slip by, as these "false negatives" can lead to fines and penalties.

An effective review process will eventually identify false positives and allow them to proceed, but reviewing large numbers of transactions is time consuming and expensive. The added burden of reviewing false positives also can introduce fatigue and increase the risk of individuals not recognizing a real positive.

Organizations therefore should look for several important properties and capabilities in their filtering software. At the simplest level, the software should be able to screen new customers and retroactively screen existing customers when new people and entities are added to watch lists or when customer data changes. It also should be able to screen financial messages in real time and meet the throughput, resilience and recovery requirements of mission-critical payments.

To be truly powerful and effective, however, screening software should employ:

- "Fuzzy matching" techniques, which are sophisticated algorithms for identifying sanctioned people and entities, despite accidental or deliberate misspellings that obscure their true identity
- Control of unstructured data and comparison with structured data
- Native language capabilities to scan and interpret all foreign alphabets and scripts and transliterations
- Know your customer capabilities to provide identity verification and risk assessment
- Algorithms that provide rapid, real-time scanning of data
- Configurable scan settings and rules that enable fine-tuning to improve accuracy and achieve the organization's unique risk profile

The result is processes that deliver the lowest false positive rates in the industry.

Know your customer

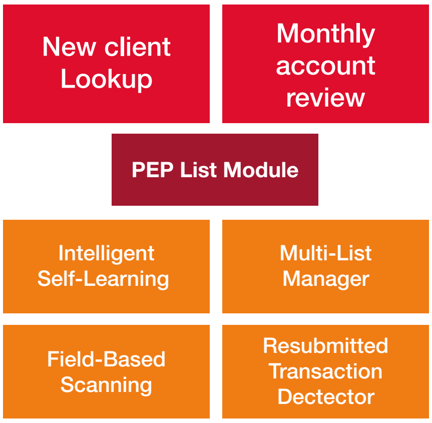
In this era of increasing digital transformation, there are two views to consider regarding know your customer (KYC). First of all, it is important to understand the customer's view. A recent Reuters survey on the impact of global changes in KYC regulations reveals that a lack of sufficient human resources and increasing regulatory change are top concerns among nearly 800 financial institutions that responded to the survey. In addition, a parallel survey of these financial institutions' corporate customers found that 89% had not had a good KYC experience, and 13% had changed their financial institution relationship as a result.

Second, there is the bottom line view. Global surveys also reveal that KYC costs and complexity are rising, which is having a negative impact on respondents' businesses. While financial firms' average costs to meet their obligations are $60 million, some are spending up to $500 million for KYC and customer due diligence compliance.

Both financial firms and their corporate customers agree that strengthening KYC procedures puts strain on onboarding processes and customer relationships. The time, for example, to bring a new customer on board was 22% more last year than the year before, and it is expected to increase an additional 18% over the next year. Further, 30 percent of corporate customers report that the time to bring new customers on board was longer than 2 months. Of these, 10% claim an onboard time in excess of four months, and that they have, on average, 8 different interactions with the bank during the process.

Sophisticated technology is one important pillar to successfully fulfilling the heavy prerequisites of KYC. A platform thus must include ad-hoc screening and due diligence, as well as a batch for regular monthly customer account KYC due diligence.

KYC-Due Diligence



Both real-time and batch capabilities need to include features like a politically exposed person (PEP) list module (PEP-screening requires special monitoring such as a four-eyes check for ongoing customer relationships), and, again, integrated intelligent self-learning (ISL). If ISL is integrated with the KYC processes and provides a learning filter rather than a static filter it can significantly reduce false positives and provide efficiency gains without narrowing the size of the net.

Intelligent Self Learning can provide:

- Increased productivity by reducing manual intervention and eliminating processing interruptions
- Minimized operational risks by achieving a balance between checking blocked accounts and maintaining continual transaction processing
- Implementation of risk assessments against terrorist lists, sanctioned entities, politically exposed people and other risk groups
- Reduced false positive alerts by as much as 70% without impacting negatively the level of filtering, resulting in fewer manual checks, more effective compliance operations and significant cost savings

Suspicious activity monitoring:

Suspicious activity monitoring is a broad field for banks and businesses to cover as policies, procedures and processes, as well as overall compliance with statutory and regulatory requirements for monitoring, detecting and reporting suspicious activities, need to be assessed.

Suspicious activity reporting forms the cornerstone of the reporting system in the U.S. It is critical to the ability of countries to use financial information to combat terrorism, terrorist financing, money laundering and other financial crimes.

Within this system, FinCEN and federal banking agencies recognize that, as a practical matter, it is not possible for a bank to detect and report all potentially illicit transactions that flow through the bank.

Key components include the following:

- Employee identification
- Law enforcement requests
- National security letters
- Transaction monitoring
- Surveillance monitoring

Suspicious activity monitoring, which involves the analysis or investigation of unusual patterns of actions, is a major issue and covered by important regulations, such as the Bank Secrecy Act. It is based on the detection of agreed upon deviant cases sought by regulators or the police. It is a good example of why flawed traditional approaches need to be modernized by minimizing silos and why different business processes need to be synergized.

Maintaining silos, grey zones occur and, just as importantly, synergies are wasted. The synergy benefits also impact functional units such as internal controls, compliance and investigation, risk management, and anti-fraud management. CGI's Protect the Bank architecture offers great potential for synergy and cost reduction. Suspicious activity monitoring should include features such as the following:

- High-performance, real-time, scalable risk engine
- Integration interface in the form of an adapter module
- Predictive analysis module, with advanced statistical methods, visualization and modeling
- Data visualization and analytical process results
- Case management
- Reporting
- Analytical data warehouse (profile and behavioral characteristic preparation are included)

Fraud

"Fraud" is defined in the Oxford dictionary as "wrongful or criminal deception intended to result in financial or personal gain."

A "fraudster" is defined as "a person or thing intended to deceive others, typically by unjustifiably claiming or being credited with accomplishments or qualities."

These definitions show how wide the field is and how many components it contains. Fraud is a criminal human behavior. Contrary to some acts of terrorism, it is always committed by a human being. Thus, soft skills and forensics are key elements to prevent a fraudster from being one step ahead.

Know your enemy: what does a typical fraudster look like?

The process of identifying a typical fraudster by recognizing certain types of behavior has a long and problematic history. Research has shown that convicted fraudsters have similar personal and professional backgrounds, but of course this research applies only to fraudsters who have been caught. Different profiles might apply to more successful fraudsters who manage to evade detection.

Robust internal business controls will assist in identifying potential risks at the earliest opportunity and, of course, the visible detection of fraud and strong law enforcement can be a key deterrent.

Research also shows that an effective way to prevent fraud is to remove excuses used to justify offending. This can be achieved by making policies and procedures that govern behavior across the business and making them accessible and understandable to all, at every level, thus making it easier for workers to act honestly. Explaining the benefits of compliance and the penalties for non-compliance can help prevent staff from arguing that "no one suffers as a result of fraud" or that "the government can afford it."

Finally, evidence available from fraud profiling can be used to identify those with the highest risk of offending, such as sales staff far from home. They can then be provided with additional support and advice to help them to act honestly.

As with other areas of financial crime control, intervention at the earliest opportunity has considerable benefit in terms of reducing losses and harm, and enabling otherwise productive employees to continue to pursue risk-free patterns of work.

What else is needed to make the institution secure?

As has been shown many times recently in the press, good processes and solutions cannot provide the total answer without the right people, skills and awareness across the business.

It's all about people: Training, skills and awareness

Banks and businesses must employ staff with the skills, knowledge and expertise to carry out their functions effectively. They should review employees' competence and take appropriate action to ensure they remain competent for their roles.

Vetting and training should be appropriate to employees' roles. Strict compliance depends on skilled professionals who use compliance technology and evaluate each alert generated. The process for reviewing alerts requires different levels of expertise—from first level triage to the demand for in-depth knowledge of multiple sanction regimes at the highest levels.

Each alert must be reviewed quickly and be assigned an accurate risk score to speed transactions and minimize costs while also assuring full compliance. Tailored training has to be in place to ensure staff knowledge is adequate and up to date. All new staff must be trained on financial crime from the time they join and the training should focus on practical dimensions. Finding and retaining the right people for this function is critical.

Hiring and background check procedures

Reference checks are no longer formalities. Employers must take references seriously because they know invaluable information is obtained from what is shared (and what is withheld). This also is a primary reason for choosing references wisely. Understanding best practices for the reference check process is important.

Effective hiring procedures are crucial. They ensure the identification of people with valuable skills, such as analytical thinking and an inquisitive mindset, as well as an ability to work collaboratively with colleagues across the organization when deciding whether to approve a transaction. Prospective employees must be able to grasp complex processes and spot hard-to-see relationships about people and groups. New sanctions programs, such as sectoral sanctions targeting specific regions like Russia, also may require expertise in new languages.

Typical background checks include the following:

- Employment history checks (verification of past employers)
- References (personal or professional)
- Social networking and Internet searches
- Drug testing (may be required in some countries during and after the hiring process)
- Credit checks (becoming more common; check of a candidate's credit report)
- Pre-employment screenings (general knowledge to perform the job; aptitude or psychological screening)

Background checks may vary based on local legislation and risk profiles.

Employee workshops and training

Ongoing training ensures that employees understand and can effectively apply the requirements of new financial crime regulations. This training should be standardized and provided at least annually to refresh skills and knowledge. Organizations also should take advantage of industry forums and other events that offer opportunities to exchange ideas, keep abreast of changing tactics of terrorists and criminals, and learn best practices from other industry experts.

Additional training is needed with respect to communications with third parties and clients. A single phrase from an employee or manager has been known to cause important reputational damage. In this context, social media can be a challenge, as channels like Twitter serve as channels for communicating corporate messages to the markets.

Employee awareness

Training employees and staff fosters increased awareness and sensitivity for spotting fraud patterns. This is key because whistleblowing systems are only as good as the contributions of internal staff. Quality training, alongside mature processes, are important elements of a well-functioning whistleblowing system.

Frequently, staff does not know how to detect a suspicious transaction in the workplace. They need awareness of the common clues indicating certain funds may be laundered or funneled into a terrorist organization, as well as of other potential sources of financial crime. They need a broad overview of anti-money laundering, terrorism financing, sanctions, anti-fraud management, general definitions, common techniques and the broad legislative framework for detecting and reporting illegal activity. This also covers globally recognized procedures for mitigating the risk posed by money laundering and terrorism financing.

Additionally, as criminals become more sophisticated, spotting potential insider threats require relying on a mix of technology and people underpinned by good awareness.

Personal career development

Career development and succession planning help create a strong and enthusiastic pool of compliance professionals able to prevent any type of financial crime. Banks and businesses should identify the critical roles on their compliance team and define the required qualifications and skills. With this information, it is possible to put in place a program for professional development and establish desirable career paths within the organization. Succession planning will keep key positions filled.

Change management support

Change management support helps ensure the organization understands and leverages new technologies and processes to strengthen and streamline the activities for combatting financial crime.

Together, these activities will minimize compliance risks by ensuring the organization maintains the high quality human capital necessary to meet the challenges of today's rapidly changing compliance landscape.

Smooth and streamlined processes as a key to sound compliance

Smooth and streamlined processes are a key to sound compliance. Again, there are many facets to consider, and a single linear view of processes is not sufficient as nearly all essential products and employees are linked to a common goal. All regulated organizations face the same situation: regulatory pressure amid budget restrictions, rising costs for compliance, and exponentially rising data, both in terms of volume and diversity.

A main problem is data quality. A study revealed that 75% of data is unstructured. This promotes new types of financial crime. Some of the reasons include the following:

- Fragmented processes
- Evolving environments
- Lack of automation
- Lack of integration
- Lack of focus on key issues

In times of transformation, it is more important than ever to have one streamlined digital process that covers the entire process cycle.

Sound technology is one key factor to avoid labor and resource intensive efforts. With the integration and automation of integrated financial crime platform technology, best practices are enabled and automated. A case management, or Command and Control Center helps organizations increase their return on investment by combining operational and technological know-how, focusing key resources on financial crime and its risks.

Conclusion

The conclusion of this white paper can be summarized in two sentences. First, implement a holistic approach for combatting financial crime through a combination of technology and interdisciplinary know-how. Second, an efficient framework consists of an integrated financial crime platform that breaks silos and includes big data analytics, integrated self-learning and case management.

Banks that do not transform their financial crime architectures will struggle to succeed at regulatory compliance. Those that do transform will be able to dramatically reduce their run costs, freeing up resources and funds to invest in digital transformation elsewhere in the institution.

Compliance is much more than just the name of a functional unit. Employees and management can demonstrate their integrity through the sound financial crime management. Forward-thinking banks and businesses create opportunities in the area of compliance for increasing customer acquisition and retention. And, this becomes a strong differentiator for them in a competitive market.

Adopting an integrated approach to financial crime management helps to ensure the broadest possible coverage, improves return on risk and compliance investments, and enhances reputation.

With Protect the Bank (PTB), CGI offers a comprehensive, compliant approach to financial crime management, helping clients to establish smooth digital processes at reduced costs, while ensuring the institution is protected from financial crime.

About the author

Elif Morgenroth is the head of CGI’s anti-money laundering, anti-fraud management and financial crime management practice in Germany. Before she joined CGI in Germany, she was employed by two of the “Big Four” accounting firms, as well as an attorney. She has many years of experience within the finance sector, as well as other sectors, and was involved in the establishment of CGI’s Protect the Bank solution.

Elif covers all financial crime topics, with a specialized focus in forensics, criminal justice and internal investigations.

About CGI

With more than 20 years of experience in developing and delivering cost-effective financial crime solutions, CGI's 500+ compliance and security experts apply their deep understanding of the complex regulatory landscape to help leading organizations around the world fight financial crime.

CGI has been supporting and shaping the financial services market for nearly 40 years. We were behind the original design for the SWIFT interbank network and have worked with 70% of the world's top financial institutions, including 8 of the top 10 global banks.

We work as a partner, not just a provider. Through a consistent, disciplined and accountable delivery approach, CGI has achieved an industry-leading track record of on time, within budget projects. As a result, our average client satisfaction score for the past 10 years has measured consistently higher than 9 out of 10. We are helping financial institutions, including most major banks and top insurers, reduce costs, increase efficiency and improve customer service.