On the case:
Mitigating emerging financial crime risks through enhanced case management

September 2015

Survey data provided by

NICE ACTIMIZE

pwc
Making the case for centralized case management

The magnitude and the impact of financial crime are well documented, but a new age of criminal activity is dawning. Financial criminals are exploring sophisticated methods to further their pursuits and outmaneuver organizations trying to stop them. In this increasingly complex risk landscape, financial institutions are discovering that their historically siloed approach to combating financial crime is putting them at a significant disadvantage relative to nimble, innovative wrongdoers. These institutions increasingly require solutions that can offer holistic views of risk across their organizations allowing them to connect the dots across both transactions and investigations in near real time. A centralized case management system can help companies do just that. By taking a more panoramic and risk-based approach to identifying financial crime, the financial community can prevent criminal activity before it happens—and do so with far greater efficiency.

The impact of emerging risks

Despite greater regulation, the volume of financial crimes being reported globally continues to rise. Suspicious Activity Report (SAR) filings alone have grown more than 220% in a 10-year period. An environment of greater control in long-standing areas of financial crime has pushed financial criminals to explore less-supervised areas such as virtual currencies and peer-to-peer lending, and it has contributed to the emergence of new forms of financial crime such as trade-based money laundering. As these new risks arise, so does the need to respond to external investigative bodies to protect against the financing of drug cartels, terrorism, human trafficking, and other threats.

Financial institutions have invested significant amounts of resources in the enhancement of internal controls, but with numerous organizational silos responsible for fighting financial crime, it is becoming increasingly difficult—and expensive—to achieve a holistic view and effectively manage risk.
To gain a better understanding of the specific challenges financial institutions face in adopting these less-fragmented and more-integrated approaches, NICE Actimize sponsored a survey of financial services executives that focused specifically on the global state of enterprise risk case management. The survey found that among financial institutions with at least $60 billion in assets (defined for this paper as “large”), 53% had more than 10 analytic and/or detection systems and 31% had more than 20 (Figure 1). These disparate activities not only affect efficiency but also prevent financial institutions from uncovering hidden relationships that help identify crime (Figure 2).

**Figure 1: Financial institutions have a large number of analytic/detection systems**

Approximately how many analytic and/or detection systems does your organization have in place to support financial crime and compliance needs?

- 22% of large companies have fewer than 5 systems
- 25% have 5 to 10 systems
- 22% have 11 to 20 systems
- 31% have more than 20 systems

Source: NICE Actimize 2015 Case Management Industry Survey

**Figure 2: Siloed systems across regions and functions make it difficult for organizations to manage risk**

Companies are challenged to recognize related activity and adequately assess risk across financial crime units.
**Financial Intelligence Units working to keep up**

Recognizing their exposure (see sidebar Top drivers for unifying financial crime), financial institutions continue to evolve their Financial Intelligence Units (FIUs) by consolidating the efforts of disparate financial crime teams that instead take a more centralized crime-fighting approach. From the early days of essentially providing an oversight capability to aggregate and disseminate information, FIUs are evolving into centralized shared-services organizations for all fraud or anti-money laundering or, in emerging cases, into one central FIU for all financial crime investigation. (See Origin and evolution of the FIU.)

**Top drivers for unifying financial crime**

The NICE Actimize survey found that the top three drivers for unifying financial crime and compliance risk management are reputational damage protection; transparency and regulatory scrutiny; and financial implications of crimes and fines. More than half (56%) of respondents said they’re concerned about protecting their company’s reputation. Beyond the potential negative press attention is the risk of more permanent reputational damage as seen by the public at large.

With regulator focus on transparency of processes and controls, financial institutions have become motivated to increase the visibility of investigations from initial alert triage through evidence gathering and case management, which is greatly simplified by the implementation of centralized case management. There is no regulation that says financial institutions have to look at all transactions centrally, but those with centralized case management systems can standardize processes and be more responsive to regulators’ needs.

Finally, the financial implications of crimes and fines are primary motivators for 45% of survey respondents to unify their financial crime risk management. Recent high-profile fines have reinforced the need for broader sharing of intelligence, especially cross border. Upwards of $184 billion in fines for regulatory violations has been paid by 46 big banks and two nonbanks since 2009, with 174 cases currently outstanding. For comparison, the gross domestic product of New Zealand is roughly $184 billion.

**Effective FIUs are enabling financial institutions to integrate disparate sources of data for conducting investigations and for more easily implementing enhancements to their company’s controls over financial crime.**


**Origin and evolution of the FIU**

Financial Intelligence Units (FIUs), or Financial Crime Intelligence Units (FCIUs) date to the early 1990s, when central government agencies were established as units to receive, analyze, and disseminate financial information with a view to combat financial crime. Recognizing the importance of international cooperation in the fight against money laundering and the financing of terrorism, many FIUs joined together to form an international network. Known as the Egmont Group, this network shares financial crime intelligence and collaborates in the areas of information exchange, training, and the sharing of expertise.

Even though no regulatory directive mandates financial institutions to implement FIUs, many banks began setting them up following the lead of government agencies. The charters of many of the early FIUs were to serve as hubs for gathering and disseminating financial crime intelligence. As they continue recognizing the value of having centralized information available for analysis and investigation, FIUs are evolving to help their organizations take smarter approaches to financial crime prevention. For example, FIUs are serving as a central body that standardizes processes across lines of business, geographies, and financial crime domains—such as anti-money laundering (AML), fraud, bribery, corruption, sanctions, tax evasion, and cybercrime—so as to increase efficiency and effectiveness.

Effective FIUs are enabling financial institutions to integrate disparate sources of data for conducting multiple financial crime domain investigations and for more easily implementing enhancements to their company’s controls over financial crime. Rather than taking a reactive approach focused primarily on producing SARs and sharing them across jurisdictions, FIUs are becoming more proactive by trying to address thematic and horizon risks such as trade AML and human trafficking, by making better use of intelligence, and by developing more-analytic capabilities.

There is no blueprint for an FIU within a financial institution. However, common operating model functions include a breadth of capabilities, from risk identification to investigations, watch-list management, and horizon scanning (Figure 3).

---

**Figure 3: FIU evolution**

From passive administration

- Suspicious report received from internal controls/business units
- Investigation conducted to evaluate risk and reporting requirements
- Suspicious Activity Report (SAR) or Currency Transaction Report (CTR)

To proactive enforcement

- FIU uses a combination of technology-enabled analytics and coordinated intelligence gathering to determine areas of risk.
- Investigations conducted into risk scenarios through data gathering and communication with front-line staff.
- Evaluation of risk and remediation plan determined. This will include suggestions to tighten internal controls or P&P impacts.
- Relevant action can be employee disciplinary action, SAR/CTR/other regulatory reporting and business policy changes.
The NICE Actimize survey showed that 75% of large financial institutions access at least four systems and 25% access six or more to obtain the data needed to investigate a typical work item or alert. For example, in a standard investigation, an investigator might access a customer relationship management system to look up the relationships of the person under investigation. The investigator would look in another system to see whether the person or any related parties have sanctions against them. The investigator may then check other data sources for negative views on the person or related parties. All of that information resides in different units in the organization, but the investigator must pull it all together, which is time-consuming. In the survey, 67% of large institutions reported that investigators spend more than 30% of their time on manual activities and that more than 25% spend more than 50% of their time on manual processes (Figure 4). In such an environment, as surveillance systems generate more and more alerts, FIUs are striving to meet the dual objectives of:

- Increasing efficiency by making decision-based investigation and resolution more automated by automating the first-level review of alerts or giving investigators both the information and a recommended decision to make the process more efficient
- Increasing effectiveness by developing consistent procedures across investigative teams and making automated decision recommendations for certain types of investigation. Such increased rigor and standardization further investigators’ ability to demonstrate that they are using high-quality, and robust processes while streamlining investigations.

Figure 4: Investigators often spend significant amounts of time on manual processes

In thinking about a typical financial crime or compliance investigation, approximately what percentage of time per month does an investigator spend on manual processes?

Source: NICE Actimize 2015 Case Management Industry Survey
An analysis of the return on investment from the use of a centralized case management system shows that the return can substantially outweigh cost and effort. (See sidebar Quantifying the benefits of centralized case management.) Centralizing a particular function, such as AML, can create operational efficiencies that result from reduced overhead and information technology (IT) costs (see case study Centralized case management can increase efficiency and reduce costs). Centralization may take the form of a single global investigation team or multiple regional teams located in less-expensive labor markets with SAR filings still taking place in the compliance function of the pertinent country. Increased investigative effectiveness can reduce financial crime losses and lower the risk of fines and reputational damage while improving regulatory responsiveness.

Enterprise risk case management: Not a panacea but a lifeline for investigators

The implementation of a centralized case management system that not only automates low-risk activities but also provides insights for human investigators on complex, suspicious incidents can be game changers in financial crime risk management. Investigators save time and therefore increase efficiency by accessing a single platform that stores information centrally. Obtaining information from a single source enables investigators to cross-leverage that information more efficiently and effectively, eliminating duplication of effort and accelerating investigations. When the same person or when related parties are triggering alerts across different types of financial crime (AML, sanctions, fraud), geographies, or channels (phone, ATM, branch), that type of activity becomes more readily detectable. Further, the platform provides a basis for analytics that can propel financial institutions to proactively prevent financial crime before it happens.

Centralized case management can increase efficiency and reduce costs

A global bank with eight systems for online, deposit, and credit fraud was struggling to efficiently investigate fraud alerts. Without consistency across the eight systems and without a holistic view of fraud risk, the bank was unable to provide timely and accurate customer-centric fraud management. By implementing a centralized case management solution, the bank developed a standardized, best-practice approach to sharing enterprise data. As a result, it became able to reduce false-positives from 250:1 to 5:1 and reduce information technology team costs by 50%.

An analysis of the return on investment from the use of a centralized case management system shows that the return can substantially outweigh cost and effort.
Quantifying the benefits of centralized case management

As with many business decisions, it is essential to understand, categorize, and quantify the potential benefits of enterprise case management technology in order to create a compelling business case for technology investment.

From an operational perspective, combining functions such as fraud and AML into a single tool creates substantial efficiencies by reducing request-based overhead and greatly expediting processes (see case study Providing a more complete view of fraud links throughout the organization increases accuracy). Enabling the case management system to normalize alert risk scores and prioritize the alert saves investigators time, which can be redirected to focus attention on high-risk alerts. Functionality within the technology directs the alerts to the right investigator based on the type of risk.

Case management systems can also create efficiencies beyond transaction-monitoring alerts and SAR filings. For example, adding Financial Crimes Enforcement Network Section 314(a) requests to the system helps ensure the request reaches the right investigators. The single customer view that often accompanies the implementation of centralized case management can greatly reduce the time investigators spend in manually accessing disparate systems or in requesting data from other divisions. That reduction not only results in operational efficiencies but also increases investigational effectiveness, because data is less likely to be overlooked.

In aggregate, proper implementation of enterprise risk case management technology provides substantial tangible business benefit in four key categories as follows.

<table>
<thead>
<tr>
<th>Impact</th>
<th>Sample Benefits</th>
</tr>
</thead>
</table>
| **Operational efficiency** | • Consistent, streamlined processes and automation reduce time spent on manual processes, reduce the number of false-positive alerts, and increase teams’ productivity.  
                          | • Consolidation of financial crime investigation reduces overhead costs.  
                          | • Integration of resources into less expensive labor markets reduces labor costs.  |
| **Information technology efficiency** | • Consolidation of multiple hardware platforms reduces ongoing expenses of technology procurement and maintenance.  
                          | • A single centralized tool reduces the cost and speeds the process of adapting systems in response to regulatory changes, internal process changes, and emerging threats.  |
| **Investigative effectiveness** | • Increased effectiveness in identification and investigation of suspicious activity results in lower costs associated with financial crime loss (lack of deterrence, unidentified fraud, inefficient fraud-event response).  |
| **Regulatory risk reduction** | • Effectively enabling groups responsible for organizational compliance and risk case management reduces the risk of fines, consent orders, and reputational damage.  |

Providing a more complete view of fraud links throughout the organization increases accuracy

A bank had identified gaps in its online fraud coverage and was unable to correlate links between systems. It merged its fraud and AML technologies into one enterprise case management system, automated the fraud detection and AML compliance processes, and created unified risk profiles. The results were an enhanced view of fraud links across multiple channels and increased accuracy and productivity achieved through automation.
Despite the clear benefits, many organizations have not seized the opportunity to upgrade entrenched processes and systems. The NICE Actimize survey showed that just 19% of large financial institutions are able to fully investigate a work item, alert, or case within a single solution—without manually accessing other systems.

At the same time, financial institutions have huge expectations that in the next 24 months they will fully integrate processes and systems based on a unified technology architecture and data model. Today 14% of large financial institutions report fully integrated models, but almost three times that number (39%) expect to be fully integrated within 24 months (Figure 5).

Case management systems can also create efficiencies beyond transaction-monitoring alerts and SAR filings.

---

**Figure 5: Financial institutions expect a greater level of integration between their processes and systems within 24 months**

Which of the following most accurately describes your organization’s financial crime risk management processes and systems?

- **Fully integrated:** Processes and systems based on a unified technology architecture and data model
  - In 24 months: 39%
  - Today: 14%

- **Semi-integrated:** Processes and systems with some level of alignment and data sharing, but not fully integrated
  - In 24 months: 50%
  - Today: 53%

- **Completely disparate:** Processes and systems with little or no integration
  - In 24 months: 6%
  - Today: 28%

Source: NICE Actimize 2015 Case Management Industry Survey
Evolving case management to outpace financial crime

Financial institutions will require new ways of thinking about case management if existing and emerging FIUs are to realize greater efficiency and change the way investigations get done. In our experience, leading financial institutions are following an evolutionary thought process and taking approaches to case management that are defined by three implementation waves (Figure 6).

**Leading financial institutions are following an evolutionary thought process**

**Figure 6: Waves of case management implementation**

- **Wave 1: Core Case Management** (centralized processes and tools)
  - Anti-money laundering
  - Entity screening/Sanctions
  - Case management system

- **Wave 2: Enterprise Case Management** (holistic customer view)
  - AML transaction monitoring
  - Fraud detection system
  - Know Your Customer (KYC)
  - Case management system
  - Regulatory reporting
  - Governance reporting

- **Wave 3: Predictive Modeling and Intelligence Mining**
  - Intelligence mining
  - Predictive modeling
  - External data sources (structured and unstructured)
    - Social media and other news
    - Intelligence task forces
    - Financial crime alert services
**Wave 1: Core case management**

Core case management capabilities (Figure 7) enable financial institutions to more efficiently and effectively manage workflows. A well-designed workflow allows users to perform everyday tasks more efficiently. The aid of more automation and sophisticated policy rules improves visibility into questionable behavior and makes the triggering, triage, and assignment of alerts by AML or fraud monitoring more streamlined. This process is supported by the integration of all relevant data from transaction-monitoring systems, fraud systems, and customer systems into the case management system so that such data is easily accessible as part of an investigation. A system that enables a financial institution to maintain various high-risk lists (customer, beneficiary, country, etc.) brings further intelligence to investigations. Audit trails let other case managers, supervisors, and auditors quickly view a case and understand each action taken. A robust audit trail is of increasing importance because prosecutors are turning their attention to individual employees—as well as the corporations where they work—when investigating corporate crime.4

**Wave 2: Enterprise case management**

Once core case management capabilities are in place, a financial institution can focus on bringing together all relevant client and transaction data sources to enable case investigation and provide a 360-degree view of exposure across AML, fraud, sanctions, advanced due diligence, and so forth.

Companies are gaining traction in integrating their customer data streams to develop a single customer view that can support risk management and compliance. (See PwC’s white paper “Chasing a vision: Pursuing a single customer view for financial institutions.”) Yet more can be done to truly transform their ability to identify suspicious behavior and meaningfully streamline regulatory compliance processes.

Once data has been consolidated into a single case management system, financial institutions are able to apply analytics to all case dispositions in order to monitor metrics (suspicious activities, rate of false-positives, etc.) and more proactively identify trends that can lead to greater efficiency and effectiveness.

---

*A system that enables a financial institution to maintain various high-risk lists (customer, beneficiary, country, etc.) brings further intelligence to investigations.*
Wave 3: Predictive modeling and intelligence mining

Today, financial institutions that have achieved wave 2 are industry leaders in case management, yet under the pressure to excel in financial crime investigation, these will soon become requisite capabilities. Looking forward, the next wave in capabilities involves using advanced analytics and technology to enhance case management (Figure 8). Many of these enhancements may be internal, such as using statistical risk scoring to drive risk-based workflow and thereby facilitate prioritization and routing of cases to increase efficiency. However, the real difference comes from using analytics for greater intelligence mining of external sources.

An intelligence platform pushes beyond an enterprise view of data to gather and share networks and other sources outside the enterprise. Screening for negative news becomes integrated within banks’ financial crime operating models, and the FIU becomes a Center of Excellence for handling externally available unstructured data. Incorporating intelligence from external sources—such as joint money-laundering intelligence task forces (human-trafficking task force, international trade task force, terrorist-financing task force, corruption task force, etc.) and financial crime alert services—enriches the information base for more effective decision making. And aggregating both internal and external sources provides investigators with a more comprehensive view of a customer’s relationship and makes internal watch lists and high-risk lists more robust and dynamic. With integrated information in hand, financial institutions can also share information more easily with regulatory parties and facilitate information sharing among various authorities.

Figure 8: Enhanced case management through IT and analytics
Using a central case management system can be a catalyst for centralization of lines of business or geographies into common standard procedures and system architectures. It could mean, for example, that several countries use the same system and share information but that teams reside in their existing countries. Or a centralized investigation team could replace country teams and reside in a lower cost region. Many organizations are electing to create a centralized financial crimes office or a situation room, to which AML, fraud, and trade surveillance report and to which they can respond in real time to emerging events and ongoing or residual risks.

**Overcoming implementation challenges**

Industry, regulatory, and data-specific knowledge are required to make the implementation of a new case management solution effective enough to truly transform the work of an FIU, allowing investigators to manage their caseloads without sacrificing quality. Case management solutions need to be tailored to an institution’s specific risk profile, its suite of products and services, and its specific data environment. The integration process that individual FIUs follow will vary in complexity and direction depending on these various factors as well as size and organizational structure. In all scenarios, transformation will take time, and a phased approach is necessary.

Following an agile methodology will help secure return on investment along the way. In such an environment, capabilities are prioritized according to user requirements and value. Functional software is delivered quickly—in weekly sprints that enable the visualization of requirements. Frequent deployment of code allows business users to see the end product as it gets developed and to confirm that the requirements are being documented correctly. Frequent deployment also leads to high levels of collaboration between business and development, thereby increasing the quality of the end product by improving understanding of requirements.

The use of accelerators can make the integration of data less onerous. Distributed analytic solutions virtually eliminate the need for large-scale data migration by accessing data where it resides, which makes for a much more flexible, on-demand approach to performing analytics. Such solutions seek out data across systems according to specific criteria, and rather than pull the data into a centralized repository and park it there, the solutions apply rules and analytics to the data at the source. Instead of creating a daily feed of all client information into a case management system, this approach could allow the system to pull only relevant client data as users or the system needs it.

Other new accelerators are essentially making the process of merging data sets together significantly easier by simplifying the process—from IT personnel who write mountains of code based on their understanding of business needs to business analysts who look at the full set of data themselves and perform data quality adjustments as needed.
Data privacy and security

As companies determine their data strategies and integrate data sources to support centralized case management, they must come to recognize the constraints imposed by privacy concerns and data security. To support the completeness and integrity of information and to track data lineage, once data sources have been determined there must be procedures in place that direct how and where information should be maintained.

Data privacy laws can restrict the sharing of information between designated countries. Tight collaboration across geographies is fundamental to understanding the ways regulations and privacy laws vary from country to country, how data and information management practices may differ from business unit to business unit, and how the very roles of risk and compliance functions may vary according to region.

Customer contracts can cause data privacy concerns, too. For example, terms of service may state that information will not be shared with a third-party affiliate, including or excluding affiliates that are considered the same company. To hurdle that obstacle, banks can typically issue new terms of service. Guiding the data integration with this type of detailed knowledge and global coordination will help resolve a financial institution’s specific business problems without introducing unnecessary complexity and effort.

Sustainability

Transformation through centralized case management requires strong governance both during implementation and post-implementation. During implementation, a rigid change control process and proper executive leadership will help complete the project on time, on budget, and in scope. Post-implementation, ongoing governance is needed to provide direction when new risks, policy changes, new business units, new regulations, new solutions, and changes within the investigative unit arise.

Getting the jump on financial criminals

Fraudsters and other financial criminals both outside and inside the organization are savvy when it comes to exploiting the gaps that exist between financial crime prevention systems that focus only on a single channel or line of business or region. In addition, inconsistent processes and lack of an enterprise view create areas of financial crime and regulatory risk. Facing skyrocketing alert volumes and SAR filings, financial institutions need to become willing to rethink their approaches to case management. The potential return on investment from centralized case management is significant, because siloed organizational structures, inconsistent processes, and disparate data have created opportunities for tremendous gains in efficiency and efficacy.
Endnotes


Acknowledgments

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.
To have a deeper conversation about enhancing your case management system, please contact:

John Sabatini  
Principal  
PwC  
(646) 471 0335  
john.a.sabatini@pwc.com

Chad Hetherington  
GVP & General Manager,  
Case Management  
NICE Actimize  
(212) 994 3943

David Choi  
Principal  
PwC  
+ 44 (0) 207 212 1809  
david.d.choi@uk.pwc.com

Donna Weiss  
Director, Product Marketing  
NICE Actimize  
(212) 574 3637  
donna.weiss@niceactimize.com

Vikas Agarwal  
Principal  
PwC  
(646) 471 7958  
vikas.k.agarwal@pwc.com

Kevin Dalvi  
Principal  
PwC  
(312) 298 2896  
kevin.dalvi@pwc.com

Devesh Desai  
Director  
PwC  
(646) 471 0501  
devesh.desai@pwc.com