COMPLIANCE WEEK
THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK, AND COMPLIANCE

Achieving a Unified View of Financial Crime Risk

By Joe Mont

Increased regulatory scrutiny and the sting of billions in fines and penalties resulting from misconduct have prompted many financial firms to pour money into their compliance programs—investments that may be in vain without a unified view of risk.

A recent poll of 90 financial institutions conducted by NICE Actimize, a financial crime solutions provider, underlines the siloed environment many banks still operate in. According to the survey, 53 percent of financial institutions with at least $60 billion in assets have at least 10 different detection systems. Another 31 percent have more than 20.

"Systems and processes that are not linked make it hard to aggregate and consolidate data," says Michael Atkin, managing director for the EDM Council, a non-profit trade association founded by the financial industry to elevate the practice of data management. That means financial institutions don't have a full view of their risk or insight into opportunities, he says.

Increasingly, however, banks recognize the need to achieve a unified view of risk, driven by a confluence of regulatory scrutiny, high-profile fines and penalties, and the need to protect against reputational damage. "We're seeing more and more financial institutions wanting to achieve a unified view of risk," says Chad Hetherington, global vice president at NICE Actimize.

The overall goal is to link existing systems and processes to gain a horizontal view of operations, get a consolidated view of risk, and reduce operational costs. "It is not possible or reasonable to rip and replace these systems," Atkin says. "The better approach is to harmonize the data and normalize the messaging processes."

Some banks are trying to achieve that unified view of financial crime risk by establishing financial intelligence units (FIUs). "FIUs are serving as a central body that standardizes processes across lines of business, geographies, and financial crime domains—such as anti-money laundering, fraud, bribery, corruption, sanctions, tax evasion, and cyber-crime—so as to increase efficiency and effectiveness," PwC said in a white paper accompanying the NICE Actimize data. "FIUs use a combination of technology-enabled analytics and coordinated intelligence gathering to determine areas of risk."

The purpose of FIUs at global banking giant HSBC, for example, is "to identify and investigate significant cases, trends, and strategic issues related to financial crime risks and share relevant data and intelligence across the group," HSBC said in a recent post on its website. Other banks that have established FIUs include Royal Bank of Scotland, Standard Chartered, and Barclays.

Even with an FIU in place to centralize processes, gaps in financial crime analysis persist, putting banks at risk. The NICE Actimize survey showed that 75 percent of large financial institutions access at least four systems, and 25 percent access six or more, to obtain the data needed to investigate a typical work item or alert.

"For example, during a standard investigation, the investigator would most likely check the customer relationship management system, a separate sanctions screening system, a separate transaction monitoring system, and a fraud surveillance system that holds additional activity details about an individual," says John Sabatini, advanced risk and compliance solutions leader at PwC.

Centralized Case Management

The solution for many banks is to implement a centralized case management system so investigators can access 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," PwC said in its white paper.

Sabatini says a direct correlation exists between centralizing risk mitigation and centralizing a company's IT and data platforms. "What we've seen in the market is that companies are taking a phased approach to achieve this target operating model," he says. "It begins with an assessment of your current environment and a firm understanding of your key systems and data feeds."

"Once you establish a data universe, you can begin to see where centralization can reduce duplicative processes and optimize current systems by leveraging data that the organization already has, but may not necessarily have been using in a certain context," Sabatini says.

Implementing a centralized case management system typically takes place in three phases:

Core case management. "Core case management capabilities enable financial institutions to more efficiently and effectively manage workflows," PwC said. Automation improves visibility into questionable behavior and makes the triggering, triage, and assignment of alerts by AML or fraud monitoring more streamlined.

Implementing a centralized risk management program is not as daunting as it may seem. "Most companies already have the tools, systems, and data to make advanced risk management a reality," Sabatini says. The goal is to take all that data from transaction-monitoring systems, fraud systems, and customer systems, pour it into a case management system, and make that data easily accessible during an internal investigation.

Additionally, Sabatini says, developing consistent procedures across various investigative teams—financial crime, trade surveillance, fraud, corporate security, and more—and making automated recommendations for specific types of investigations can increase overall compliance effectiveness.

Enterprise case management. Once core case management capabilities exist, financial institutions can then focus on culling relevant customer and transaction data sources to "provide a 360-degree view of exposure across AML, fraud, sanctions, advanced due diligence, and so forth," PwC said.

By integrating customer data streams to develop a single customer view, financial institutions can better support risk management and compliance, "so that they can tie all the bits and pieces of data together and they can see all the various relationships that exist," Hetherington says. Sometimes different business units share the same customer, "and yet they will treat them differently from a financial crime perspective," he says.

That's problematic, especially where regulators are going into banks today and identifying where different business functions share the same customers. "They're asking them, 'Why did you handle this activity this way, and this activity another way?' When the institution doesn't have a good answer, it's a problem, and it really puts the institution at risk," Hetherington says.

Predictive modeling and intelligence mining. "The next wave in capabilities involves using advanced analytics and technology to enhance case management," PwC said. In this way, data gathered and shared from sources outside the company are used, and screening for adverse media becomes integrated within financial crime operating models.

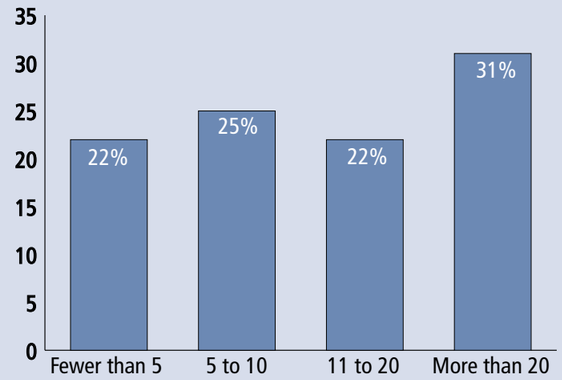
Some banks today are trying so-called "in-memory computing" technology, like SAP HANA, which helps companies to detect patterns and analyze massive amounts of data "with very little effort in a very short timeframe," says Falk Rieker, global head of banking business at SAP.

Incorporating intelligence from external sources—such as money-laundering intelligence task forces and financial crime alert services—makes 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," PwC said. "With integrated

> "Once you establish a data universe, you can begin to see where centralization can reduce duplicative processes and optimize current systems by leveraging data that the organization already has, but may not necessarily have been using in a certain context."
>
> John Sabatini, Advanced Risk and Compliance Solutions Leader, PwC

DETECTION SYSTEM STATS

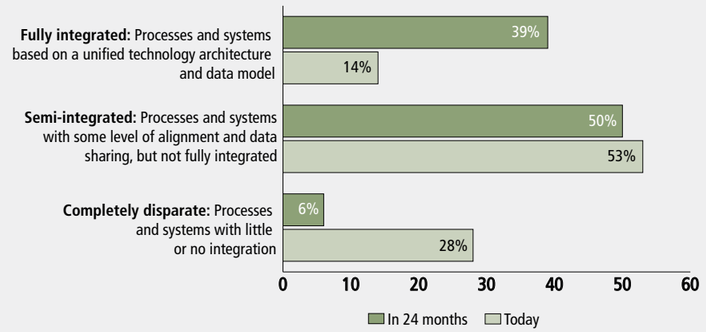
Approximately how many analytic and/or detection systems does your organization have in place to support financial crime and compliance needs?



Source: Nice Actimize.

CRIME RISK MANAGEMENT SYSTEMS

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



Source: Nice Actimize.

WWW.COMPLIANCEWEEK.COM » 888.519.9200
Reprinted from Compliance Week, January 2016

information in hand, financial institutions can also share information more easily with regulatory parties and facilitate information sharing among various authorities."

Data management as an objective does not happen overnight, "because it requires coordination and alignment among organizations that have many, many priorities to manage," Atkin says. He advises approaching data management from a "practical point of view," meaning incremental delivery, having in place well-structured governance mechanisms, and having a clear understanding of business requirements.

Siloed organizational structures, inconsistent processes, and disparate data systems create risks for all financial institutions. Having in place a centralized case management system is one way to reduce financial crime risk and the inevitable aftermath of significant fines and penalties. ■