www.pwc.com

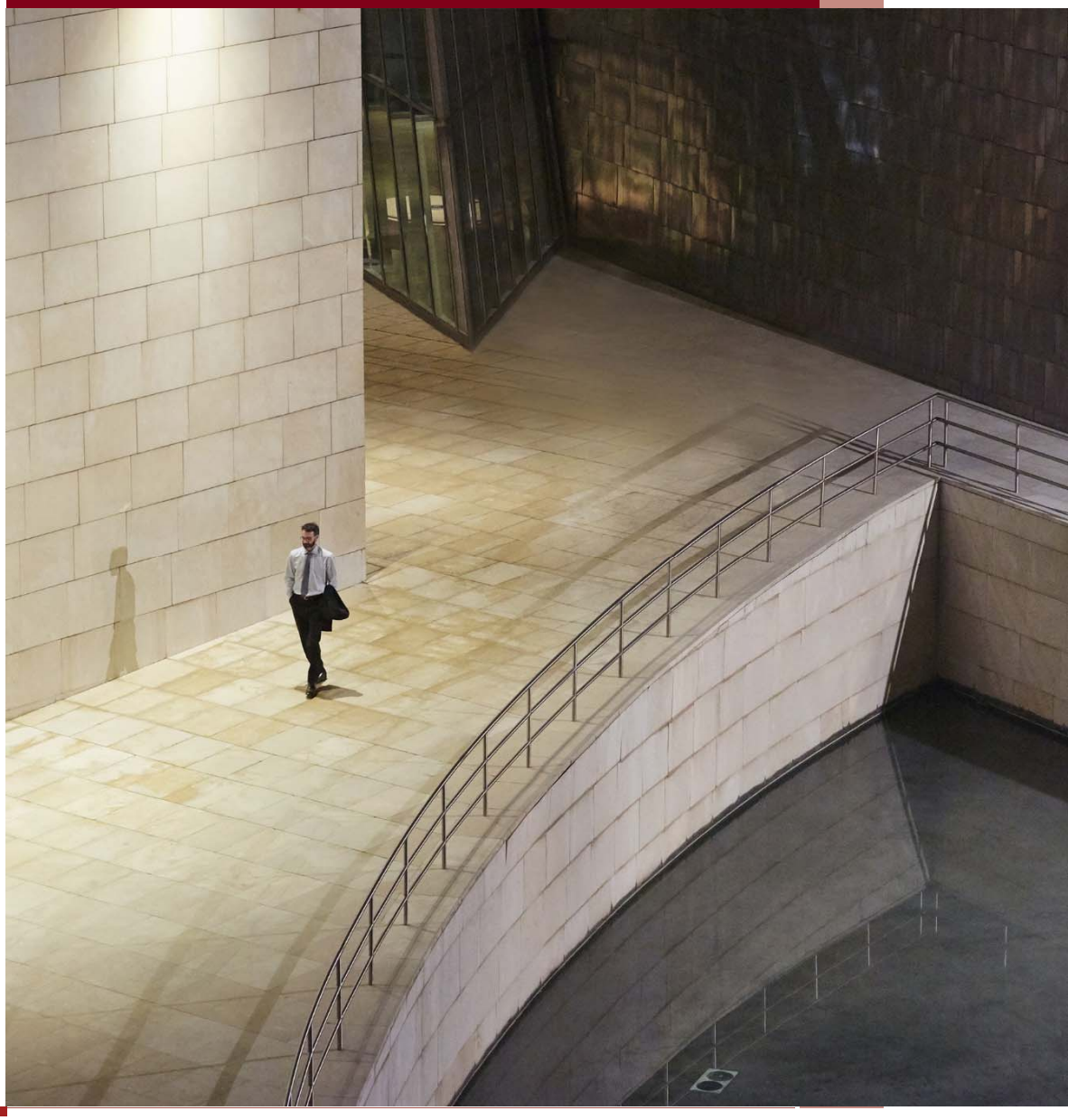
Manual transition

Transforming financial crime investigations through automation

December 2016

Survey data provided by

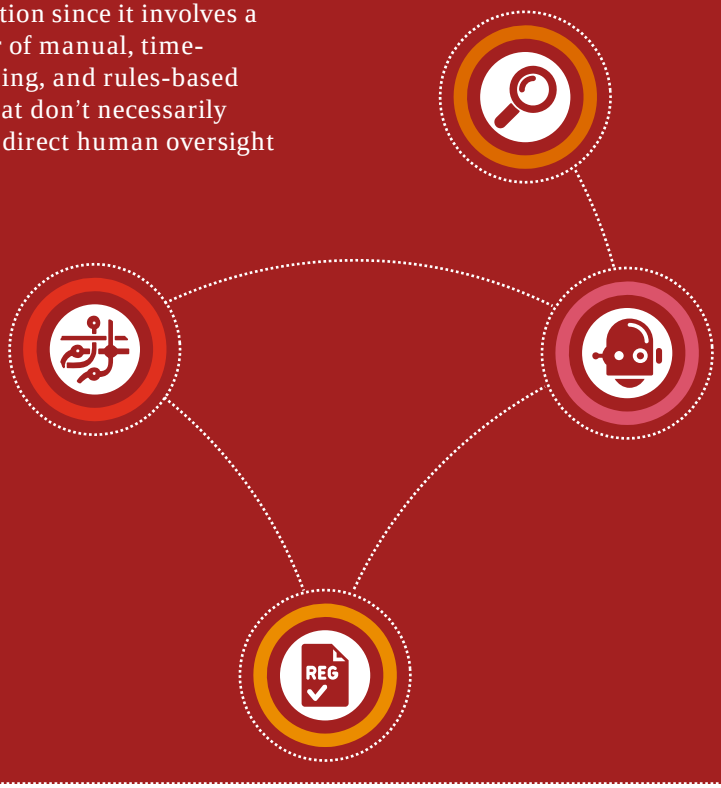
NICE ACTIMIZE



pwc

What you need to know

- Financial crime regulations and law enforcement initiatives can add significantly to the costs financial institutions must bear, driving a need for technology-enabled controls and compliance processes
- However, a staggering 87% of respondents to a recent survey by NICE Actimize said their organizations' financial crime risk management processes and systems today are, at best, somewhat efficient, with investigators spending significant time on manual activities
- Fortunately, the investigative process itself is fertile ground for automation since it involves a number of manual, time-consuming, and rules-based tasks that don't necessarily require direct human oversight
- To make their investigations more efficient, financial institutions are pursuing a range of automation strategies involving data acquisition, consolidation, and analysis; alert ranking and prioritization; alert routing and investigator nudging; and automated system health checks, among others
- Taken together—and combined with other techniques, such as streamlined regulatory filings—these approaches can help financial institutions transform their financial crime investigation programs and empower investigators without replacing them



Executive summary: Clear mandate, unclear path

The magnitude and breadth of the financial crime epidemic are staggering. According to the United Nations Office on Drugs and Crime, global money-laundering transactions involve roughly $1 trillion to $2 trillion annually.[1] Meanwhile, almost half of financial institutions around the world have fallen victim to economic crime in the past 24 months, according to respondents to PwC's Global Economic Crime Survey 2016.[2]

There is also wider collateral damage to consider, including business disruptions, regulatory fines, legal fees, investments in remedial measures, investigative and preventive interventions, and, critically, damage to morale and reputation, all of which can significantly impact long-term business performance.

Indeed, compliance team headcount at some of the world's largest banks has more than tripled in recent years, with no signs of retrenching. The competition for qualified talent is intense, and control function hiring and retention challenges are exacerbated by the need to adjust to a changing workforce, which millennials will start to dominate by 2020.[4]

Faced with such challenges, many financial institutions have invested in enhancing their internal controls over financial crime while concurrently driving resource productivity. But others are still only beginning to transform their financial crime compliance programs. Where should those institutions begin? Creation and/or centralization of financial intelligence units is a good place to start.

Some have turned to automation, which offers enormous potential to improve the efficiency and efficacy of financial crime-related operations. But because of the sensitive nature of risk and compliance-related processes, many financial institutions have made only limited progress in applying automation to financial crime prevention.

Fortunately, some lower-risk automation opportunities can yield significant benefits, and one area where a number of leading financial institutions have focused their efforts is on streamlining their investigations processes.

For instance, automating the acquisition, integration, and analysis of data and facilitating regulatory filings can help address a major source of manual effort. Combining these techniques with more complex approaches to automation such as alert risk-scoring, intelligent alert ranking, alert routing, and system health checks can help financial institutions transform their financial crime investigation programs.

In an environment marked by skyrocketing costs of compliance and increasingly complex forms of criminal behavior, financial institutions are turning to automation to enhance controls and improve efficiency.

New regulations and law enforcement initiatives focus on mitigating financial crime threats, but they also add significantly to the costs that financial institutions must bear. The investments needed in hardware, software, and employees to keep pace with regulatory compliance are tremendous. At major banks, governance, risk management, and compliance costs can account for 15 to 20% of total operating cost, according to some estimates.[3]

Such efforts can help financial institutions efficiently identify increasingly complex forms of financial crime and support regulatory compliance while reducing redundancy across different functions and geographies.[5] But where should organizations that have already begun integrating their financial crime compliance efforts look next to enhance controls while managing costs?

[1] Money-Laundering and Globalization, United Nations Office on Drugs and Crime, https://www.unodc.org/unodc/en/money-laundering/globalization.html.

[2] http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html.

[3] Matthias Memminger, Mike Baxter, and Edmund Lin, "You've Heard of Fintech, Get Ready for 'Regtech,'" *American Banker*, September 7, 2016, http://www.americanbanker.com/bankthink/youve-heard-of-fintech-get-ready-for-regtech-1091148-1.html.

[4] Bhushan Sethi, Dietmar Serbee, Kurtis Babczenko, Jeff Lavine, et al, *Under control: Pooling control functions talent in financial services*, PwC, October 2016, http://www.pwc.com/us/en/financial-services/publications/assets/pwc-fsi-whitepaper-talent-in-control-functions.pdf

[5] For more on financial-intelligence-unit centralization, see *On the case: Mitigating emerging financial crime risks through enhanced case management*. September 2015, http://www.pwc.com/us/en/risk-assurance/publications/case-management-whitepaper-aug-2016.pdf.

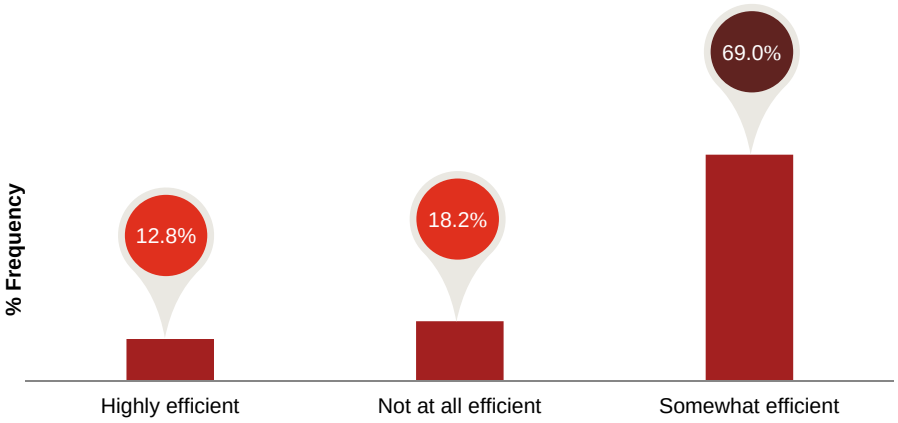
The state of inefficiency

To better understand why financial institutions are targeting investigations in particular for transformation, it is helpful to consider some of the challenges investigators currently face.

For the second consecutive year, NICE Actimize sponsored a survey of financial services executives focused on the global state of financial crime and compliance risk management.[6] The survey highlights the considerable inefficiency resident in investigative processes, and the priority that financial institutions are placing on creating efficiencies—specifically by moving to automate investigations' manual aspects.

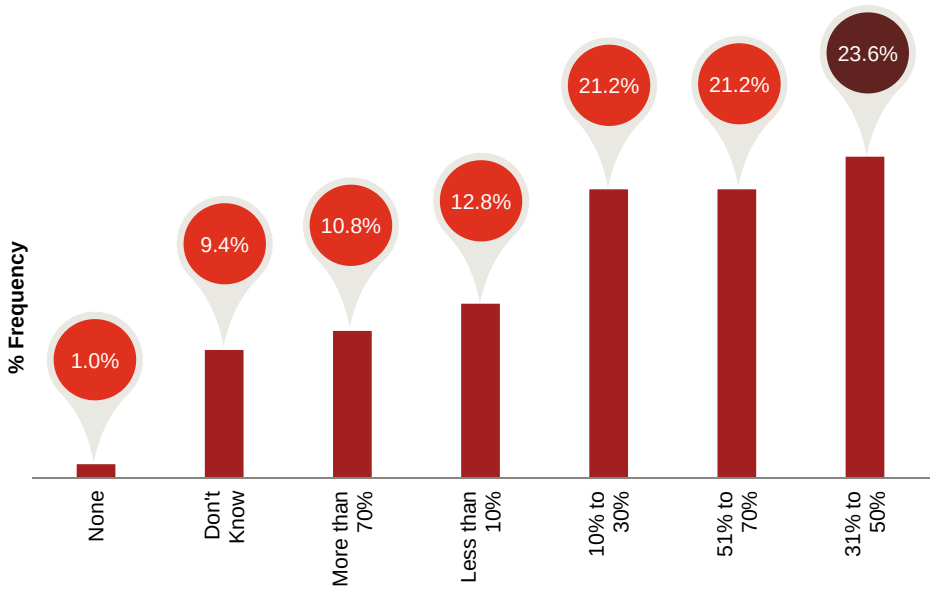
An overwhelming 87% of respondents said their organizations' financial crime risk management processes and systems today are, at best, somewhat efficient, with investigators spending significant time on manual activities (Figure 1). More than half (56%) reported that analysts spend at least 30% of their time per month on manual processes such as phone calls, emails, and collection of data (Figure 2).

Figure 1: Which of the following most accurately describes your organization's financial crime risk management processes and systems today? (Respondents could choose only a **single** response.)



- **Highly efficient:** Many processes are automated, and investigators spend the majority of their time on systems based on a unified technology architecture and data model.
- **Not at all efficient:** The majority of processes are manual, and significant efficiency gains could be made.
- **Somewhat efficient:** Some processes are automated, but investigators spend a lot of time on manual activities that could be automated. There is room for efficiency gains.

Figure 2: In thinking about a typical financial crime or compliance investigation, approximately what percent of time per month does an analyst spend on manual processes such as phone calls, emails, and collection of data)? (Respondents could choose only a **single** response.)



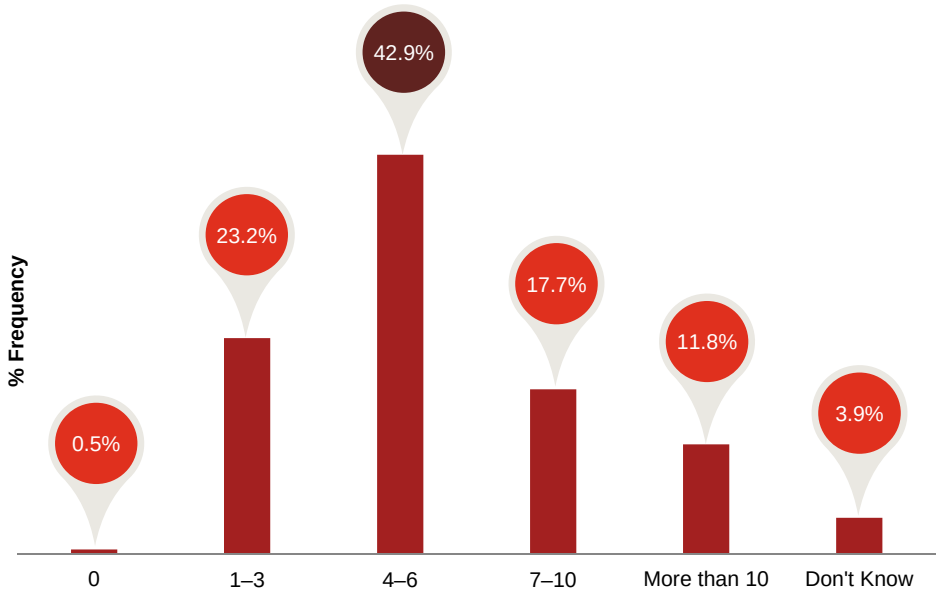
[6] The NICE Actimize survey was an online survey conducted globally in mid-2016. The 203 survey respondents represented a wide distribution of geographic locations, company sizes, and financial services sectors.

Adding to the inefficiency are the number and complexity of systems that analysts must access to complete investigations (Figure 3), which more than 40% of survey respondents cited as their greatest challenge in improving the investigation process.

Moreover, rather than becoming simpler, the environment seems to be growing more complex—particularly at large financial institutions with $60 billion or more in assets. Last year, 25% of large institutions reported accessing six or more systems to obtain the data needed to investigate a typical work item or alert. This year, 51% of large-institution respondents reported accessing seven or more.

The motivation to create more-efficient financial crime investigations is strong. According to the survey, the percentage of respondents who said they believe their financial-crime-investigation processes will be highly efficient within two years is *nearly triple* that of those who said they believe their processes are efficient today, signaling a significant drive to increase efficiency. But how will organizations get there?

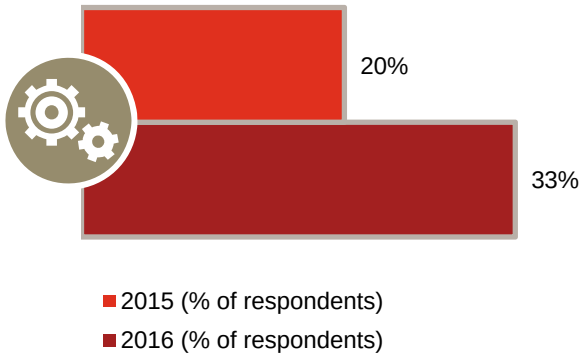
Figure 3: On average, how many systems or data sources are accessed during a "typical" financial-crime-and-compliance investigation at your organization today? (Respondents could choose only a **single** response.)



Trending in the right direction?

Despite financial institutions' efforts to improve investigation efficiency, a key survey finding reveals that the manual nature of investigations persists.

More than 50% of time per month is spent on manual processes.



The promise of automation

An estimated ***45%*** *of work activities can be automated, which could save*

$2 trillion

in global workforce costs

Robotic process automation (logic-driven software tools that apply rules to data) and digital labor are evolving quickly and have the potential to transform the way organizations execute a wide range of activities. PwC estimates that as much as 45% of work activities can be automated and that such automation would save $2 trillion in global workforce costs.[7] But for today's financial institutions—which are operating in a highly competitive market with increased pressure to improve margins now—what does automation mean in practical terms?

Digital labor is ideal for manual, time-consuming, rules-based tasks; and advances in technology have opened new ways of thinking about which work functions humans really need to perform.[8] When it comes to risk and compliance programs in particular, artificial intelligence (computing that simulates human cognitive processes) and machine learning (a form of artificial intelligence that enables computers to learn from processing large sets of data without being explicitly programmed) have created a number of exciting opportunities.

For example, robotics can assist in evaluating credit limits, determining causes for breaches in credit limits, and recommending remedial actions. Natural language processing can help with trade surveillance by monitoring trader communications for signs of suspicious behavior. Automation is also helping streamline risk reporting by checking the accuracy and comprehensiveness of underlying data before it is prepared for analysis.

With financial institutions facing pressure to increase investigation efficiency, the automation of certain aspects of the financial-crime-investigation process offers tremendous potential. In fact, it may be the only feasible way to keep up with the volume of investigations financial institutions must handle and the regulatory requirements they must meet. Automation can increase investigation speed, accuracy, and consistency and, just as important, enable investigators to spend more time on the value-added activities needed to mitigate risk.

But when it comes to automating the financial-crime-investigation process, organizations will need to decide which opportunities make the most sense given their operations and risk profile. Indeed, automating the investigation process requires a pragmatic, balanced approach that increases efficiency and satisfies regulatory expectations without introducing new or unacceptable risk to the organization.

[7] Thomas Torlone, Rodger Howell, Fanny Ip, and Anuj Mahajan, *Organize your future with robotic process automation*, PwC, 2016, https://www.pwc.com/us/en/outsourcing-shared-services-centers/assets/robotics-process-automation.pdf

[8] For instance, banks are streamlining lending by automating aspects of the loan application process and creating faster and more-efficient back-office processes, including account origination and servicing. Insurers are realizing efficiencies by automating aspects of policy and claims coding and processing. Automation is transforming finance and accounting processes by replacing manual activities in accounts payable, accounts receivable, ledger reconciliation, expense reporting, and other activities once performed by people. And marketing and lead management automation is helping drive increases in banks' pipelines of new customers. So, financial institutions are already taking advantage of automation to perform both front- and back-office processes faster, at lower cost, and with higher levels of accuracy.

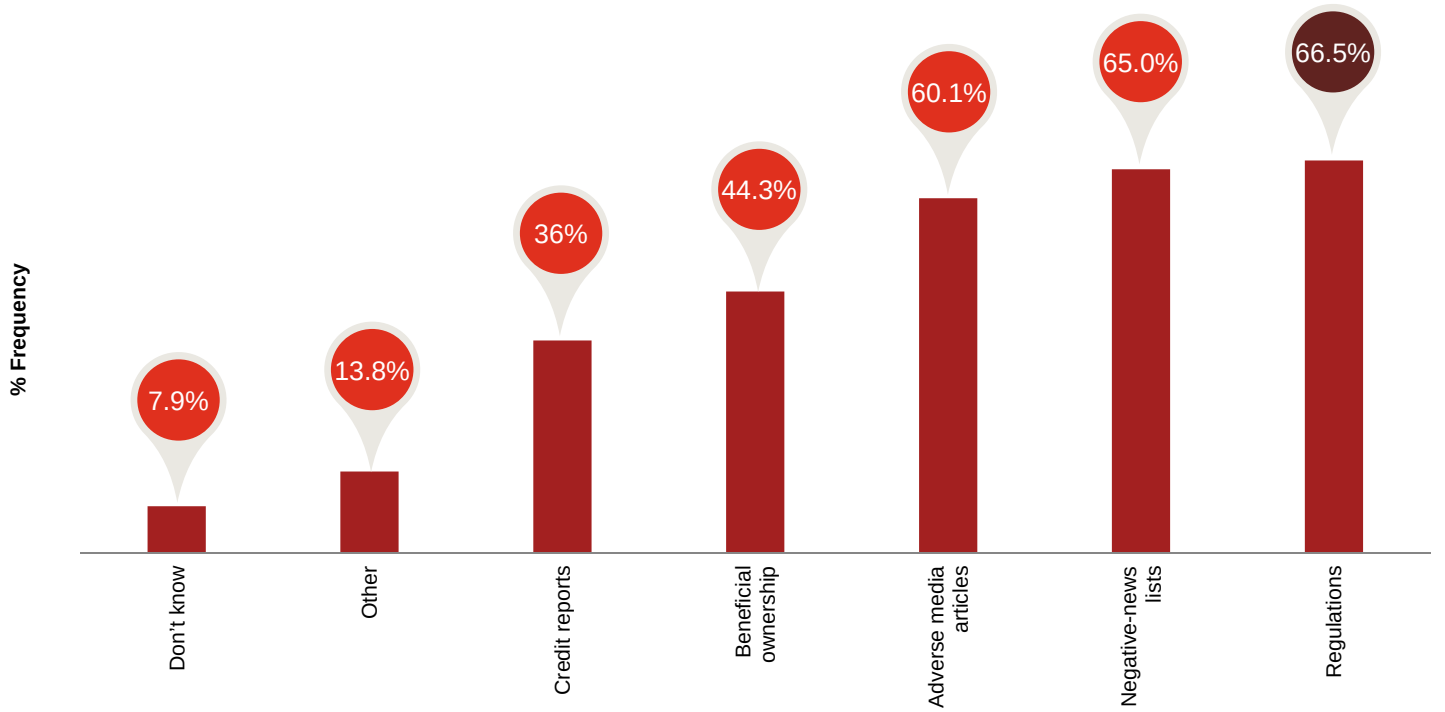
Quick wins

The most-straightforward initial opportunities for automation lie in rote, time-intensive activities that are integral to the investigative process and that serve to empower decision making without influencing or replacing the human decision itself. There are several strategies to consider in this category.

Data acquisition and consolidation

Investigators often gather data from many information sources while compiling evidence for a financial-crime or compliance investigation. They collect contextual information from internal systems containing client reference and profile data. They scour systems that may contain previous cases other control functions have handled with the entity or related parties. And they hunt through external systems for negative news or other potentially relevant facts that describe the business the entity is in, relationships the entity maintains, activities the entity may be engaged in, and more. The NICE Actimize survey found that two-thirds of respondents access negative news and regulations, and 60% also include adverse media reviews as routine sources contributing to their investigations (Figure 4).

Figure 4: What types of external, third-party, or public-domain data does your organization use during an investigation? (Respondents were allowed to choose **multiple** responses.)



When investigators do find relevant information, they must often retrieve the evidence by saving or scanning copies and must then load that evidence into whatever case management tool they use. That process introduces its own set of challenges because the types of files investigators retrieve can vary significantly. More than two-thirds of survey respondents access email services, office application programs (including word processing, spreadsheet, and presentation files), PDF files, internal transaction systems, and alert-detection systems in the course of data gathering (Figure 5). Many expand their reach much further.

Collectively, these steps can make the process of gathering and consolidating evidence extremely time-consuming. Moreover, the manual nature of the process can easily lead to errors (albeit in good faith) and introduce inconsistencies. Investigators often exhibit varying levels of proficiency when it comes to researching and gathering relevant content, and different investigators may consult different search engines, use different keywords, and take different overall approaches, resulting in the discovery of information that may be materially inconsistent.

The lack of a standardized approach introduces the possibility of variable quality across investigations, which can raise regulatory scrutiny. For those reasons, it's not surprising that respondents to the NICE Actimize survey cited evidence gathering as the area they would most benefit from automating (Figure 6).

Figure 5: What internal systems or file types does your organization use during a financial-crime-and-compliance investigation? (Respondents were allowed to choose **multiple** responses.)

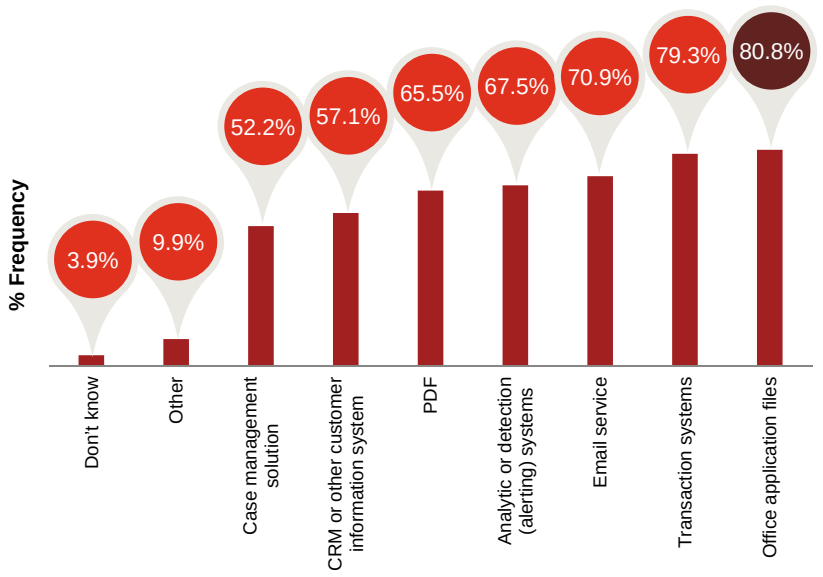
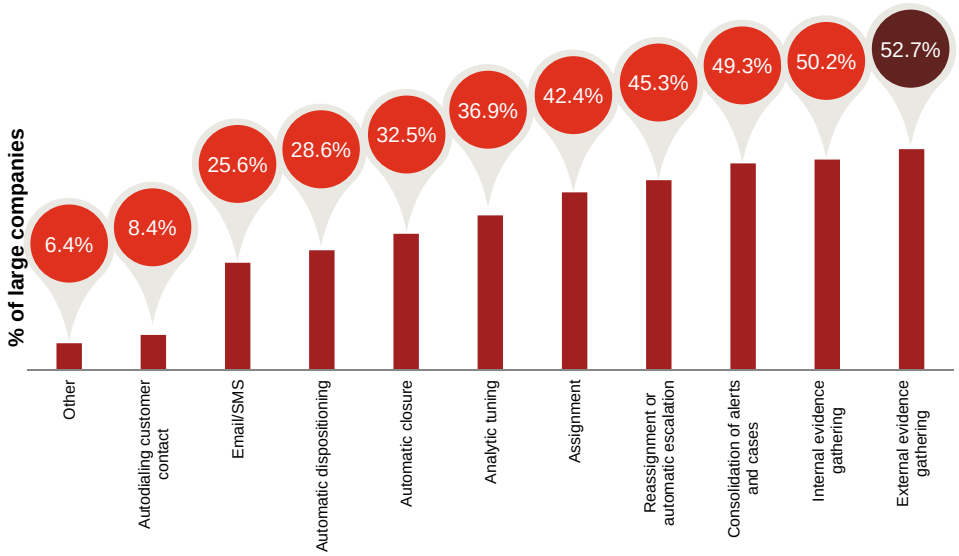


Figure 6: What triage and investigative activities that involve "human touch" today do you feel your organization would benefit from automating? (Respondents were allowed to choose **multiple** responses.)



The rote nature of evidence gathering, combined with the manual intensity of current processes, makes it a prime candidate for automation. The automation of evidence gathering can create a consistent approach while dramatically reducing the time spent in collecting and consolidating information. By leveraging application programming interfaces provided by various information sources, case management platforms can help financial institutions manage evidence from within a single system, thereby reducing the need to toggle in and out of different programs to retrieve and load data. Systems also enable the investigator to import a multitude of file types, which can dramatically cut time spent manipulating files and acquiring data (Figure 7).

Reduced toggling can yield significant savings

If an investigator spends just 10 minutes a day toggling in and out of software to retrieve data, and if that task could be automated, he or she would save approximately 40 hours over the course of a year. For a 10-person team, that equals roughly 2.5 person-months saved by reduced toggling.

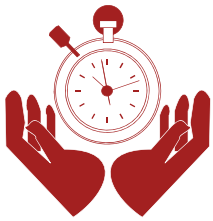


Figure 7: Representative case management system inputs and outputs

Automating data gathering and consolidation represents a significant opportunity to streamline the investigative process due to the sheer number of inputs that can flow into a case management system.

Source: PwC

Making connections

Another quick-win strategy for automation goes beyond data acquisition and consolidation to drawing connections between relevant data points. As data gets loaded into the case management system, it can be automatically tagged to an investigation. For example: typically, an investigator would manually identify how evidence is related to an investigation, such as by its relevance to the person, account, or entity under investigation.

But such tagging or linking of relevant data points does not require human involvement. Moreover, the same engine that makes the initial connection can also identify relevant relationships—such as shared accounts or companies—with names that appear in the evidence. And visualization tools can consolidate and run reports on those connections, enabling the investigator to determine what is relevant and what is not.

Such initial mapping of potentially relevant connections can be a critical component in the analysis of an investigated party's history and relationships, which is a significant stage in the investigation process. But, somewhat surprisingly, only 30% of respondents to the NICE Actimize survey report applying analytics to financial-crime-and-compliance investigative data to automate steps within an investigation, which suggests a significant opportunity to enhance current processes. The automation of basic analyses—such as frequency of customer and counterparty reference in negative news or changes in credit ratings—can give the investigator a sense of risk factors for developing a profile of the multiple dimensions of risk.

More-sophisticated use of analytics also brings greater intelligence to the investigation by uncovering trends, correlations, and relationships that may not be obvious to the investigator.

For example, there may be correlations between negative news regarding the entity under investigation and related individual subjects who appear in alerts in the bank's various control systems. Or consider this example: A bad actor hacks into a customer's checking account, which creates a cybersecurity event. That same bad actor attempts a wire transfer to syphon funds from the compromised account, creating a fraud event. Neither of the events causes a money-laundering alert for the bad actor, but it may be relevant that a party *related to* the bad actor is under anti-money-laundering investigation. Automation can help connect all of those dots and thereby give the investigator a more holistic view of the potential involvement of all parties under investigation. The system then displays the relationships through visual link analysis to support the investigator in determining the appropriate disposition (Figure 8).

Figure 8: Connecting the dots through automated link analysis

Source: PwC

More-efficient lookbacks

Lookback reviews occur for a variety of reasons, from lapses in monitoring or investigative controls to suspicions of financial crime and/or possible related regulatory breaches. A large lookback can involve millions of transactions, making it nearly impossible to complete without some level of automation. There will always be a significant manual component to this effort, but the automated risk scoring and ranking of historical alert data and investigation outcomes can accelerate the work and support a risk-based approach to the lookback. For example, statistical alert-risk scoring models can help investigators rank alerts in the lookback process and winnow down the number of alerts that require manual review.

This type of alert-risk scoring can take into consideration a wide range of factors. It can look at the riskiness of the customer and counterparty, drawing from existing customer due diligence information, geographic risks, or external lists. It may also consider the value and the channel (e.g. cash, wire, check) of the associated transactions. Further, if the lookback is focused on a specific customer, product segment, or typology (e.g. prepaid card usage or correspondent shell banks), the automated prework can be refined based on those criteria as well.

Streamlining regulatory filings

Although institutions have largely done away with paper filings for US and foreign regulators,[9] online reporting can be far from seamless. Many institutions require compliance personnel to log in to separate systems and reenter all of the information collected as part of the case. Truly integrated or embedded regulatory filing systems can pull customer, account, and counterparty details as well as information documented through investigation directly into the reporting forms for various regulatory bodies.

They can also prepopulate standard details—such as bank contact information—that would otherwise require error-prone manual entry. This functionality could prove especially useful for organizations that may have to file corresponding reports with two or more regulators—common in investigations that span multiple jurisdictions. Last, these tools can submit the filing electronically and update the status upon acceptance or send a notification if the filing gets rejected automatically for any reason.[10]

A case study in inefficiency (and a potential remedy): The RFI process

Many investigators have come to dread the request-for-information (RFI) process because it can sometimes consume days or even weeks of an investigation and lead to missed deadlines. As part of many investigations, analysts are required to reach out to relationship managers or private bankers at the customer's branch. Often, their requests involve information that only a relationship manager can answer, such as details about a client's business or the manager's investment strategy. However, in many cases, analysts' requests have to do solely with documentation, such as business incorporation forms or proof of identity. It is not uncommon for analysts at large banks to wait 14 days (out of a 30-day investigation period) for an employee at a branch to send a scanned copy of the front and back of a check. This type of data gathering is ripe for automation. For instance, the organization can relatively easily set up a process whereby the branch bank automatically feeds its documents into a repository that the enterprise case management solution accesses on a regular basis, so that the information investigators need is already available.

[9] https://www.fincen.gov/news/news-releases/fincen-marks-end-paper-sars-and-ctrs

[10] In addition to filings precipitated by an investigation, financial institutions also have to contend with both ad hoc and formal requests from regulators and law enforcement. One such example is the Financial Crimes Enforcement Network FinCEN 314(a) request that requires a bank to disclose the entirety of its relationship with a particular client. Many institutions are already tracking such requests as manual cases alongside other investigations in their case management systems. Less frequently, though, do institutions actually use all of the information already centralized in the tool to aggregate an automated report. Some institutions have integrated single-customer-view capabilities into their case management platforms, and those institutions could save a lot of time by automating their responses to these requests for analysts to review and augment as appropriate. FinCEN has processed 2,960 of such requests since November 2002, and a single financial institution may see hundreds of such requests in a calendar year; https://www.fincen.gov/sites/default/files/shared/314afactsheet.pdf.

Moving up the automation maturity curve

All of the foregoing strategies involve harnessing data and analytics to enrich case management systems by automating some of the rote activities that can unnecessarily stretch the time it takes investigators to resolve alerts. But is there a way to go even further and enable the systems to become more autonomous, to continuously improve, and to further decrease the amount of manual effort required of investigators without introducing risks?

Contextualized alert rankings

One way financial institutions can take better advantage of the data they have is by running automated queries to detect matches between new and historical alerts. That way, the system can provide a richer perspective on each new alert. The first step in such a process involves preparing historical alerts for analysis. Data visualization tools help accomplish that by enabling system managers to identify and remediate data quality issues. Historical alerts can then feed into a profiling engine that will provide context for new alerts. The system provides that context by considering each new alert as a series of attributes, which it weighs according to various risk factors.

For instance, for a certain type of alert, customer name may be more significant than, say, customer profession; or perhaps the location of the beneficiary (if it is a high-risk jurisdiction) may be more significant than the size of the transaction. The system can then determine whether the attribute matches those in prior alerts, and it can go on to rate the strength of the connection. For example, if the match is positive for customer last name but negative for customer first name, the system can automatically score that level of connection. So, the system is not only seeking connections between the information contained in current and past alerts; it is also evaluating the strength and significance of those connections.

Based on the percentage match between specific attributes and their relative importance from a risk perspective, the system can automatically generate a contextualized aggregate-risk score for each new alert, which helps in the prioritization of alerts for investigation. And the more alerts the system processes, the more information it has at its disposal to seek relevant matches, so a feedback loop gets effectively built into the system. Figure 9 offers a simplified rendering of the alert-ranking process.

Figure 9: Contextual alert ranking

Current-alert attribute	Current-alert attribute value	Attribute weight	% match with historical alert	
Account number	AC 111002	10%	0%	X
Customer name	Ned A. Sample	12%	0%	X
Customer type	Retail	25%	100%	✓
Customer business	Attorney	4%	100%	✓
Transaction type	Wire	12%	100%	✓
Transaction amount	$2,500	8%	95%	✓
Intermediary bank	Generic National Bank	4%	100%	✓
Beneficiary bank	Big City Bancorp NAM	7%	40%	X
Beneficiary name	John Doe	5%	3%	✓
Beneficiary country of residence	Belarus	12%	75%	✓
Total		**100%**	**83.6%**	✓

Alert routing

As noted, the case management system can help draw connections between entities for the purpose of ranking alerts. It can also help in identifying trends and patterns in alerts. For instance, the system can track the recurrence of certain attributes and apply thresholds to determine their relevance, such as a large number of alerts citing the same beneficiary, or a large number of similar transactions flowing to the same high-risk jurisdiction. A recurrent attribute that the system deems aberrant could raise the overall risk ranking of an alert, and the more data the system has at its disposal, the more trends and patterns it can recognize.

The system can also apply a similar logic to generate evaluations of investigators themselves. Based on a number of factors (such as investigator seniority, areas of expertise, average alert turnaround time, number of quality assurance findings, accuracy of disposition, location, and language skills), the system can create profiles of investigators that can be continuously and automatically updated. The system can use the profiles to automatically route alerts to an appropriate analyst, which can help reduce risk. For instance, if an analyst has experience in dispositioning alerts associated with a particular line of business, jurisdiction, or type of suspicious activity, the system can make that connection and accelerate delivery to that analyst. The system can even propose a hierarchy of investigators for each alert in case the top investigator is unavailable.

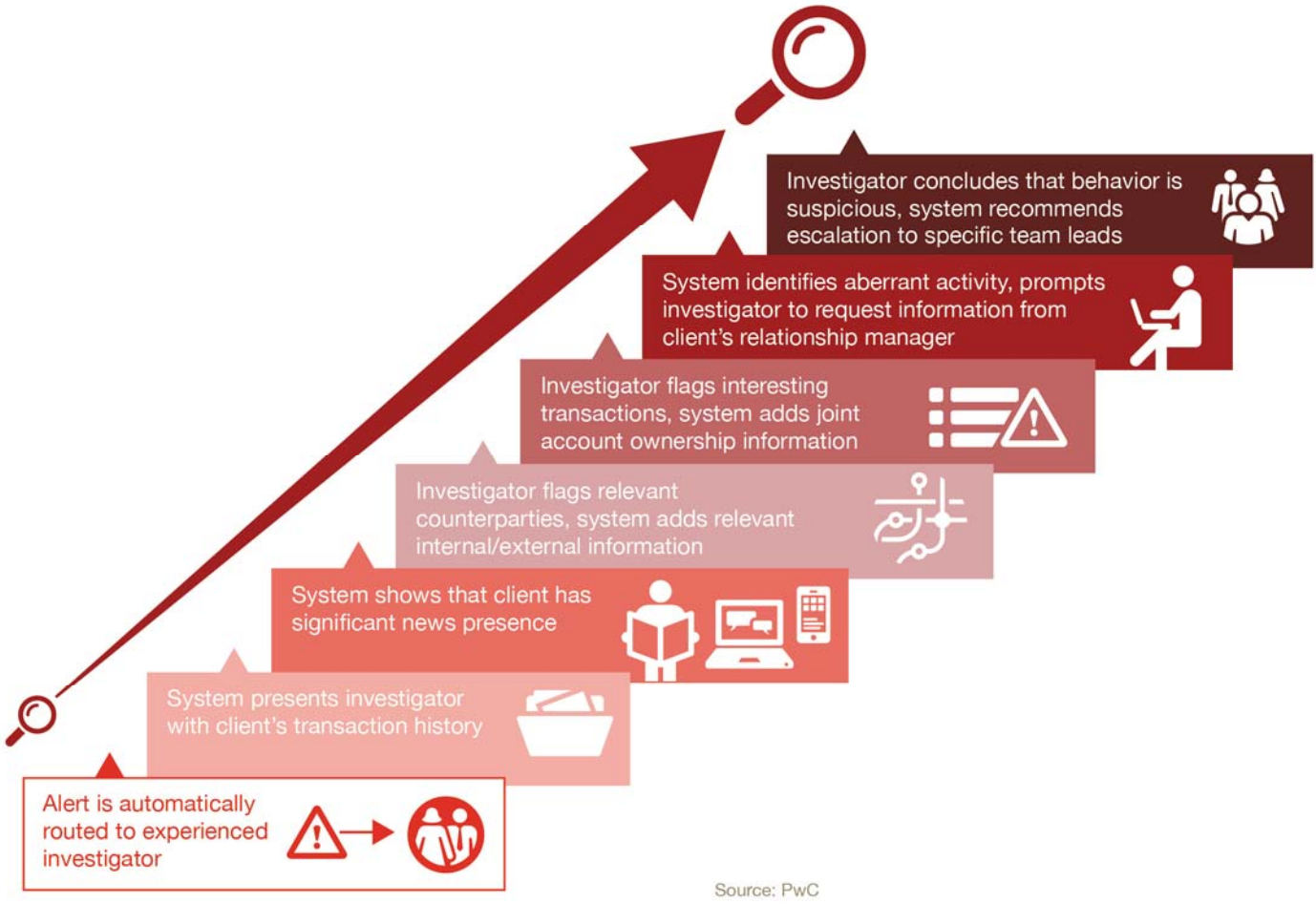
Nudging investigators

After ranking an alert and subsequently routing it to an appropriate investigator, the system can even suggest a series of next steps based on the particular attributes and risk score of the alert. If an alert that reaches or surpasses a certain risk threshold typically requires a specific response (e.g. an alert with a high enough risk score would require blocking the underlying transaction), the system can recognize the pattern and automatically suggest that investigators consider following certain steps, saving time and also reducing risk.

Moreover, the system can learn over time from previous investigations by creating historical profiles of alert types with common criteria and outcomes. Harnessing relevant information gleaned from prior investigations can be helpful to investigators who lack experience in clearing certain types of alerts.

Figure 10 on the following page depicts a representative timeline that shows how automation can enhance a typical investigation. It outlines the support a system can provide an investigator step-by-step on the path to disposition after it has routed him or her an alert.

Figure 10: Gentle nudges can enhance and streamline investigations.



Automated system health checks

As more and more data passes through the case management system, the system can run more—and more-detailed—reports to assess its own performance. For instance, the system can run automated checks to gauge whether alert productivity (the percentage of alerts that result in suspicious activity reports as opposed to false-positives) has remained stable or is seeing unexpected changes. The checks can focus on overall system productivity to determine the need to tune the system, or they can zero in on particular scenarios or groups of scenarios.

If the system detects that a scenario is not performing according to acceptable standards, it can notify a system administrator and/or compliance officer, who can assess whether the scenario needs adjustment or even removal altogether, in which case the compliance department will have documentation to support the decision. And just as the system can check its performance on an ongoing basis, it can also check the levels of productivity of investigators themselves, providing reports on alert aging, alert turnaround time, investigation quality, or other operational metrics.

Conclusion – Striking the right balance

Automating as much of the investigative process as possible is rapidly becoming a necessity for financial institutions facing rising costs of compliance combined with demands for enhanced controls. Of course, automation also has the potential to eliminate jobs. In research published in early 2016, the World Economic Forum projected that disruptive labor market changes, including the rise of robots and artificial intelligence, will result in a net loss of 5.1 million jobs in the next five years in 15 leading countries. Two-thirds of the job losses are expected to be in the office and administrative sectors as automation takes over routine tasks.[11]

However, PwC and NICE Actimize agree that the wholesale displacement of humans is unlikely when it comes to the automation of financial-crime investigations—and would also be ill-advised. Consider, for example, the disposition decision. The use of automation alone to make an investigation disposition could introduce significant risk to financial institutions.

Regulators expect investigators to develop their own risk profiles, apply expert judgment, and make sound and thoughtful decisions that they can thoroughly explain. It is difficult, if not impossible, to demonstrate those characteristics in an automated process.

Instead of *eliminating* humans, advanced analytics and the automation of rote, time-intensive tasks such as data collection can *empower* them by supplying investigators with more-meaningful information to support informed and efficient decision making. Automation can also help create structured audit trails and support more-standardized reporting, making the jobs of both compliance functions and regulators easier.

Automation should enable investigators to focus on more-relevant and critical tasks while significantly scaling the volume of investigations they process. With most financial institutions scrambling to increase their compliance headcounts as quickly as needed, this is a welcome alternative.

Four key considerations as financial institutions build their investigation automation roadmaps:

1. Develop a realistic business case that reflects implementation and maintenance costs as well as potential efficiencies and scalability.[12]
2. Differentiate between evaluating risk and collecting information that might describe risk. Focus automation on the collection of risk-based information versus using automation in decision making. Regulators support the former, but less so the latter.
3. Perform a current-state assessment to determine where operational resources are focused, and paint a picture of where investigator time is spent. Such a determination will serve to both identify priority areas for automation and set key performance indicators to monitor as automation is enabled.
4. To begin automating data collection, start with internal information collection and then include external data collection. The organization has some level of control over the information it owns, which often makes it more straightforward to automate first. Also, take a risk-based approach to prioritizing sources for the automation of data collection.

[11] "Robots, new working ways to cost five million jobs by 2020, Davos study says," Reuters, *Technology News*, January 18, 2016, http://www.reuters.com/article/us-davos-meeting-employment-idUSKCN0UW0NV.

[12] Please see Kelley Mavros, Kevin Kroen, Grainne McNamara, Tom Torlone, et al, *Payback time: Improving ROI from digital labor in financial services*, PwC, 2016, https://www.pwc.com/us/en/financial-services/publications/financial-services-roi-digital-labor.html.

To have a deeper conversation about enhancing investigations through automation, please contact:

John Sabatini
Principal
PwC
+1 (646) 471 0335
john.a.sabatini@pwc.com

Vikas Agarwal
Principal
PwC
+1 (646) 471 7958
vikas.k.agarwal@pwc.com

David Choi
Principal
PwC
+1 (646) 471 6748
david.d.choi@pwc.com

Chad Hetherington
GVP & General Manager
NICE Actimize
+1 (212) 994 3943
chad.hetherington@niceactimize.com

Donna Weiss
Director, Product Marketing
NICE Actimize
+ 1 (212) 574 3637
donna.weiss@niceactimize.com

Acknowledgments

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. 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 offers 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.