LEADERSHIP
The Chief Compliance Officer:
Renaissance Person of Today

TRENDING NOW
Emerging Developments
in Compliance

Q&A
AML Transaction Monitoring:
A Necessary, but Often Ineffective,
Component of an AML Compliance Program
A Letter From the Editors

Much has been written about the similarities and differences between art and science. In the current environment, a compliance officer needs to be a skilled performer – an artist – who interprets and is able to persuade a sometimes reluctant audience to understand and comply with myriad technical requirements – the science – of laws and regulations. It is this juxtaposition between these disciplines that we want to explore in our newest publication, *The Art & Science of Compliance*.

In this inaugural edition, we profile the Renaissance person of today – the Chief Compliance Officer. We also discuss the issues and challenges related to anti-money laundering transaction monitoring and highlight other recent regulatory developments. In future editions, we will continue to share our thoughts on the art of being a successful compliance officer in an environment of rapid change and growing complexity.

We hope that you will find this publication to be a useful resource and welcome your feedback and any suggestions you have for topics that you would like to see addressed.

CAROL M. BEAUMIER
Executive Vice President and Managing Director
Regulatory Compliance Practice

MICHAEL BRAUNEIS
Managing Director
Regulatory Compliance Practice
The days when chief compliance officers (CCOs) were primarily responsible for writing compliance policies and procedures and reviewing transactions for technical compliance with laws and regulations are largely a thing of the past. Desired qualifications of CCOs no longer emphasize the ability to quote chapter and verse of regulations. Rather, CCOs today need the ability to assess and anticipate risks and develop robust compliance management systems to manage and mitigate these risks.

In larger institutions, CCOs may be aided by senior-level executives with titles such as head of compliance risk strategy and architecture, who, among other responsibilities, develop compliance analytics and reporting. Compliance functions embedded in technology groups have also been formed in some institutions specifically to help anticipate and prioritize technology changes required to support compliance requirements.

The rapidly evolving role of a CCO now requires expanded risk management capabilities, technological savvy and the ability to forge deeper relationships with internal and external stakeholders. Coordination with the other lines of defense, including business and technology leadership, internal audit, risk management, executive management, and the board, is critical. Additionally, CCOs need to develop strong working relationships with regulators, third-party service providers, and other external stakeholders.
The rising prominence of compliance and the evolving role of a CCO are being driven by a number of factors that are mostly external to the firm. The following are among the most significant of these factors.

**Increased Regulation**
The Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA), along with its various components, marks the most significant financial regulation in the United States since the Securities Exchange Act of 1934. Many new regulations have been, and many more have yet to be, implemented by the prudential banking regulators, the new Consumer Financial Protection Bureau (CFPB), the U.S. Securities and Exchange Commission (SEC) and many others. Firms operating internationally must also contend with host country regulations and standards and a growing body of extraterritorial requirements.

In addition to the increased volume of compliance requirements, compliance officers also must deal with fundamental changes to regulatory expectations regarding how laws and regulations are addressed. The reach of consumer protection is extending beyond the typical disclosure requirements and restrictions on fees or other terms and conditions by expanding into underwriting standards (e.g., qualified mortgages and repayment ability requirements) and suitability assessments (e.g., variable insurance products and comprehensive portfolio reviews). While ensuring technical compliance with laws and regulations remains a top priority for compliance officers, compliance functions must consider more broadly whether acts or practices are potentially unfair, deceptive or abusive.

Although much attention has been paid to an ongoing increase in principles-based regulations, it should be noted that rules-based requirements continue to proliferate as well. However, financial institutions are then responsible for determining how to implement controls and procedures appropriate to the size, nature and complexity of their institutions, products and customers. Although a rules-based approach may seem more straightforward, the interpretation and customization required by firms to comply with the rules, meet the spirit of a regulation, and maintain consistency throughout the organization can make this approach more burdensome than anticipated when a regulation is first released.

**Rapidly Evolving Technology**
Technology has changed – and will continue to change – how financial products and services are developed, delivered and serviced. As manual processes are automated for efficiency purposes, the complexity of applications and systems increases, integration points become more numerous, and dependencies intensify.

The means by which institutions communicate with their customers have multiplied. More sophisticated, complex financial products and services are being offered. All of this is being powered by rapidly changing technologies. With these changes come significant compliance risks and opportunities that compliance officers must understand.
Compliance requirements, and many of the recent regulatory changes, can burden legacy systems not equipped to handle the complex requirements, necessitate the development of new or add-on systems, and require close coordination with third parties providing vendor-supported software. Technology change management processes increasingly involve compliance officers to ensure that legal and regulatory risks are addressed, required functionality is established, and changes do not affect existing compliance-related controls. Small changes needed to implement regulatory requirements can quickly add up to millions of dollars or more in technology spend for companies if not implemented effectively or on time.

At the same time, technology has an impact on compliance responsibilities. For example, the proliferation of “bring your own device” policies within the work environment and communications with customers via social media create new privacy and other technical consumer protection risks and compliance monitoring challenges for CCOs. Poor or inefficient systems design, integration and conversions increase the risk of operational errors, inaccurate reporting and delayed implementation of changes that are necessary to meet regulatory requirements. However, technology and data are also powerful tools that compliance officers can use to measure, monitor and mitigate compliance risks.

Compliance and technology are inextricably related. Compliance officers need to understand the impact of technology on business operations, but they also must harness the power of their institutions’ systems and data to do their jobs effectively and efficiently.

Scandals and Greater Scrutiny

Even after the financial crisis in 2008, the financial services industry continues to be plagued by scandals. LIBOR-rigging, the Bloomberg terminal scandal, the “London Whale” and the unraveling of additional Ponzi schemes have all made the headlines in recent years. The prevalence of such scandals and the attention they receive all drive the increased level of scrutiny from regulators, consumers and the general public that typically becomes a primary concern for the CCO.

Additional sources of increased regulatory supervision and oversight are activists, nongovernmental organizations and consumers themselves. These groups are placing greater pressure on regulators to make more rules and to ramp up their enforcement activities. Since the financial crisis in 2008, regulators have taken actions against not only the financial institutions they oversee but also the employees of those institutions that were – or should have been – responsible for internal compliance. This increased scrutiny has led generally to more attention and added responsibility within the compliance function. It is not surprising, then, that more than half of global compliance officers in the financial services industry indicate that they feel their personal liability has increased in recent months.1

Additionally, as the trend toward greater transparency continues, consumers are demanding and being granted increased access to information through social media and regulator websites, such as the CFPB’s online consumer complaint database and the Financial Industry Regulatory Authority’s (FINRA) recently enhanced BrokerCheck®. Preliminary guidance on a new requirement under the DFA will also encourage financial institutions to publicize their diversity initiatives on their websites. Ensuring the accuracy of the information that is made publicly available adds another layer of responsibility for CCOs, along with the potential for even more scrutiny.

Risk Management

The recent financial crisis exposed weaknesses in corporate governance and risk management practices, which are now subject to heightened regulatory expectations. Though the concept of risk management has largely centered on safety and soundness considerations and operational risk, regulators increasingly demand – through formal regulatory guidance and enforcement actions – that compliance be managed in a comparable manner that is integrated with the overall risk management framework of the institution. Compliance is also expected to be independent of the business and have clear access to senior management and the board of directors. Management and directors, in turn, are expected to promote a strong risk culture and set an appropriate “tone at the top” regarding compliance. These factors further support the “lines of defense” model, but also are helping the CCO to be more visible, vocal and influential in the organization.

Changing Expectations

Changes to the legal and regulatory environment, technology, and risk management expectations make the environment in which the CCO functions more dynamic and demanding than ever. As CCOs work to address the requirements of the current financial services environment, they also encounter increased expectations and numerous obstacles when addressing these issues within their own companies.

Resources: Compliance functions of all sizes face serious resource constraints given the pace of regulatory change and expanding roles and responsibilities. In addition to the individuals necessary to manage “traditional” technical compliance tasks, professionals with different skill sets are needed to take on the broader responsibilities of regulatory change evaluations, risk assessment and management, change management, product development, and issue resolution. In the highly competitive environment for talented professionals, compliance officers are searching for staff who have the qualifications to support a compliance function, but also possess skill sets that will allow the compliance function to be flexible enough to address new regulatory initiatives and requirements.

Systems and Technology: Technology is an enabler of a strong compliance management system, but it also can be a great impediment. Compliance officers face budgetary constraints for their own compliance needs, such as internal transaction monitoring systems. They must also compete with other business priorities for implementation of system controls, data retention and reporting needs. Competing priorities may mean that workarounds and manual processes are required to ensure compliance. System changes, even when tested prior to implementation, can break otherwise functioning processes due to previously unidentified dependencies. New technologies can complicate how an institution complies with existing laws and regulations. All of these factors increase compliance risks and demand attention and oversight from compliance officers who must be prepared to justify the importance of strong technology controls and change management.

Prioritizing Competing Demands: The DFA, combined with intensifying regulatory expectations and scrutiny (in the form of pronouncements and guidance from regulators and enforcement actions), is giving CCOs a stronger voice in many companies. This voice is necessary to ensure compliance initiatives are prioritized based on the risk to stakeholders and the company. Prioritizing these competing demands has grown more difficult as regulations have multiplied and the geographic reach of financial institutions has increased over the past 10 years. Compliance obligations to the workforce, senior managers, the board, consumers, third-party service providers and regulators may differ. CCOs need to prioritize their compliance obligations based on the information available to them at the time; however, they also need to be flexible enough to reprioritize compliance obligations as the environment changes.
The New Normal

Effective risk management requires identifying and mitigating known risks and anticipating future risks. As a result, compliance officers are expected to have insight into the emerging risks and compliance obligations of the firm. While you won’t likely find them in a job description, the following characteristics address the key behaviors needed for a compliance officer to survive – indeed, thrive – in this new environment.

Keep Pace: CCOs must remain current on legal and regulatory developments in all of the geographies and jurisdictions within which their institutions operate or plan to operate. In addition, CCOs must develop and maintain a deep and current knowledge of their business operations, including relevant processes and systems, products and services, customer types, vendors, and key stakeholders. CCOs also need to be apprised of environmental factors that can change how their institutions do business. Avoiding obsolescence is critical, and compliance officers must take steps to obtain and incorporate changes readily and assess and communicate compliance risks to key stakeholders. Building expertise internally within their organizations and maintaining a strong network externally are critical to keeping up with regulatory, technological and business developments.

Define Expectations: A recent Securities Industry and Financial Markets Association (SIFMA) white paper stated, “There is no single solution to reconcile the expected role of compliance professionals, as viewed by regulators and senior management, with the challenges and realities that they regularly encounter in performing their functions.”2 Clearly defining the expectations of senior management and the board for the compliance function and the CCO is a crucial step in this reconciliation process. The reverse is true as well: The CCO must assist in defining expectations for the roles that senior management and the board play in maintaining a strong compliance management system. Clearly defining expectations will enable the type of cooperative, collaborative relationships throughout the enterprise that CCOs, senior management and boards need to execute their duties.

Think Beyond the Checklist: Compliance has become more than a series of technical requirements related to disclosures and terms and conditions. Increasingly, compliance officers are required to assess risks that defy a checklist approach. No checklist will help a compliance officer determine whether a practice is potentially unfair, deceptive or abusive, or whether one practice is better than another to ensure the integrity of consumer reporting data. Compliance officers should be prepared to make thoughtful, risk-based judgments regarding compliance risks and the adequacy of their institutions’ approach to these risks.

Embrace Project Management: The volume, scope and complexity of recent and forthcoming regulatory changes increasingly require compliance officers to think and act like project managers. Leading CCOs should be comfortable participating in – and potentially leading – business process redesign, system implementation or change management efforts, and working collaboratively with their business partners to ensure that processes, technology and behaviors are sufficient to meet the compliance requirements as efficiently as possible.

Build Relationships: Each of the previous focal points of the CCO role are facilitated through stronger and broader relationship building. Relationships are vital to CCOs’ success as they work to drive change in the current regulatory environment and enhance the visibility of existing compliance efforts. CCOs must build relationships with internal stakeholders by being forthright about both compliance risks and expectations and also attuned to institutional needs. Forging, and

---

then nurturing, these relationships requires more soft skills than in prior years, including persuasion, negotiation, compromise (in the right situations) and presentation skills. Compliance officers need to be visible, they need to be part of the whole operation, and they need to collaborate throughout the company. To be exposed to management decisions in which the CCO might not have been asked to participate in years past, CCOs must readily understand business opportunities and operations, assess compliance risks holistically, and actively partner with key stakeholders.

CCOs know that compliance is not solely their job – it is the job of every employee within their institution. “Compliance” must be embedded in everything an institution does. It should be a strategic priority that is achieved through enterprise-wide collaboration. The CCO’s job has become that of a compliance spokesperson and champion, a business partner, a risk manager, and a critical decision-maker who occupies an important “seat at the table.” Getting that seat requires CCOs to master both the art and the science of 21st century compliance.
Emerging Developments in Compliance

The following provides brief introductions to a sampling of the many new or emerging regulatory issues facing financial institutions. For readers interested in learning more about these topics, we have included links to source documents.
Consolidated Mortgage Origination Disclosures

**Issue**
- Beginning in August 2015, creditors must provide a loan estimate within three days of receiving an application regarding the key features, costs and risks of the mortgage loan, and a closing disclosure three days before loan closing that helps consumers understand the costs of the transaction.

**Key Takeaway**
- Begin planning early to meet the implementation deadlines successfully.

The Consumer Financial Protection Bureau (CFPB) recently finalized rules to integrate mortgage origination disclosures required under the Truth in Lending Act (TILA) and the Real Estate Settlement Procedures Act (RESPA), fundamentally changing the manner in which these critical cost-related disclosures are provided. Effective August 1, 2015, creditors will be required to provide a loan estimate to consumers within three days of receiving an application regarding the key features, costs and risks of the mortgage loan for which consumers applied, and a closing disclosure three days before loan closing that helps consumers understand all of the costs of the transaction. Additional changes include: (1) a more narrow definition of what constitutes an application for credit; (2) clear assignment of responsibility for the disclosures to the creditor, even if the disclosures are provided on its behalf by mortgage brokers and settlement agents; (3) redisclosure of the closing disclosure and provision of an additional three-day waiting period before closing if material changes occur after it is initially provided; and (4) reduced tolerances for variances in settlement fees provided on the loan estimate. Though creditors have been provided an 18-month implementation window, the significance of the changes should not be understated. Based on recent experiences implementing changes to these same disclosures in 2008 and 2009, financial institutions must begin planning early to meet the implementation deadlines successfully and will be challenged by competing demands on compliance, operations and information technology resources necessary to implement these regulatory changes.

Source documents:
- [www.consumerfinance.gov/regulatory-implementation/tila-respa/](http://www.consumerfinance.gov/regulatory-implementation/tila-respa/)
- [www.consumerfinance.gov/blog/category/rulemaking/](http://www.consumerfinance.gov/blog/category/rulemaking/)

Debt Collection

**Issue**
- The CFPB plans to pursue rulemaking related to debt collection and increase its supervision of debt collection activities.

**Key Takeaway**
- Evaluate the sufficiency of compliance management systems related to debt collection activities for consistency with FDCPA requirements and avoidance of potential UDAAP.

The Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA) granted the CFPB the authority to regulate debt collectors and issue regulations related to debt collection under the Fair Debt Collection Practices Act (FDCPA), as well as the general ability to address unfair, deceptive or abusive acts or practices (UDAAP) related to any aspect of consumer financial products and services. While the FDCPA has been the primary statute prohibiting unfair, deceptive and abusive debt collection practices by debt collectors (who are typically third parties that collect, on a fee basis, debts originated by other financial institutions on their behalf or that acquire such debts themselves and attempt collections), the CFPB has noted that the statute does not fully address consumer protection issues regarding debt collection litigation, and changes to technology and the nature in which consumers can be (and are) contacted by debt collectors. Further, the FDCPA currently does not apply to the debt collection practices of the financial institutions that originated the debt. Heeding the calls for
expansion and modernization of the FDCPA from state attorneys general and consumer advocates alike, the CFPB has indicated that it will pursue rulemaking in 2015 related to debt collection and increase its supervision of debt collection activities (whether by financial institutions or nonbank debt collectors). Financial institutions, particularly depository institutions, should evaluate the sufficiency of the compliance management systems related to debt collection activities for consistency with FDCPA requirements and avoidance of potential UDAAP.

Source documents:
- www.consumerfinance.gov/blog/category/rulemaking/

Third-Party Risk Management

**Issue**
- Regulators have issued guidance outlining their expectations for third-party risk management and oversight.

**Key Takeaway**
- Ongoing monitoring and oversight of third-party performance are necessary, as are prompt actions to address problems identified through the monitoring process.

Financial institutions rely on third-party vendors for everything from call centers to technologies and systems to internal audit. This reliance upon third parties introduces new risks that financial institutions must manage and adds complexity to the management of other risks; however, financial institutions are still responsible for their own business and reputation, regardless of who executes the tasks. From a compliance perspective, the prudential banking regulators and the CFPB have been clear that financial institutions cannot outsource compliance with applicable laws and regulations and must actively manage the risks that usage of and reliance upon third-party vendors pose to the institution. To that end, regulators have issued guidance outlining their expectations for third-party relationship risk management and oversight, including compliance with applicable laws and regulations. Active oversight begins with vendor selection, due diligence and thoughtful contracting, whereby the vendor’s internal controls environment, past experience and reputation are considered and clear expectations about compliance responsibilities and other contractual obligations are established. Because risks to the institution remain even if the contract is clear that the vendor is responsible for a certain task, ongoing monitoring and oversight of performance is necessary. So, too, are prompt actions to address fully any problems identified through the monitoring process.

Source documents:
- www.federalreserve.gov/bankinforeg/srletters/sr1319.htm

**Issue Management and Responsible Business Conduct**

**Issue**
- The CFPB has issued guidance encouraging financial institutions to engage meaningfully in self-monitoring, self-reporting and remediation activities that could mitigate the severity of potential CFPB enforcement.

**Key Takeaway**
- Establish compliance management systems and controls to engage in self-monitoring, track identified compliance issues, implement corrective action to prevent recurrence and remediate affected consumers.

Recently, the CFPB took public action against two financial institutions for violations of certain federal consumer protection laws and
regulations. Notably, the CFPB declined to make an enforcement action against an unnamed third institution, on the grounds that this institution self-identified and remediated the issue, and cooperated fully with the CFPB during its investigation into the matter. This example is illustrative of the CFPB’s approach to handling such consumer protection per guidance it issued in 2013. At that time, the CFPB issued guidance encouraging its supervised financial institutions to engage meaningfully in activities that could mitigate the severity of potential CFPB enforcement, including: (1) regular, robust self-policing, such as thorough internal auditing, to detect early potential violations of consumer financial protection laws; (2) prompt and complete self-reporting of internally identified issues to the CFPB; (3) full remediation of consumers affected by the issue and actions to correct the underlying deficiencies that gave rise to the remediation; and (4) cooperation with the CFPB as it conducts its own discovery efforts through its examination and enforcement processes. While the CFPB cautioned that such conduct may not eliminate further enforcement activities, it may warrant favorable consideration, depending on the specific facts and circumstances. Financial institutions should establish compliance management systems and controls to engage in self-monitoring, track identified compliance issues completely, implement effective and timely corrective action(s) to prevent recurrence, and fully remediate affected consumers.

Impact of FATF Release on Financial Institutions’ Geographic Risk Ratings

Issue
- In February 2015, the Financial Action Task Force (FATF) updated its list of jurisdictions with strategic anti-money laundering (AML)/counter-terrorist financing deficiencies (CFT).

Key Takeaway
- Financial institutions should review the FATF release to determine the impact on their geographic risk ratings.

In March 2015, the Financial Crimes Enforcement Network (FinCEN) issued an advisory (FIN-2015-A0001) alerting the financial services industry to recent changes made by FATF to its list of jurisdictions with strategic AML/CFT deficiencies. FATF divides these jurisdictions into two categories:

1. Those that are subject to counter measures (Iran and the Democratic People’s Republic of Korea) or enhanced due diligence (Algeria, Ecuador and Myanmar).
2. Those that have deficiencies for which they have developed an action plan with FATF (Afghanistan, Angola, Guyana, Indonesia, Iraq, Lao PDR, Panama, Papua New Guinea, Sudan, Syria, Uganda and Yemen).

Given the importance of geographic risk ratings to customer risk assessments and transaction monitoring, timely consideration of the FATF update is warranted.

Source documents:
Q&A WITH CHETAN SHAH

Chetan Shah is a director with Protiviti’s Risk & Compliance practice, with a focus on financial services technology, including anti-money laundering analytics.

Financial institutions have an affirmative obligation to establish policies, procedures and controls designed to identify and report unusual or potentially suspicious activity. In 2013 (the last full year for which information is available), the number of Suspicious Activity Reports (SARs) filed by U.S. financial institutions continued an upward trend with more than 1,640,000 SARs filed. Assuming a typical (and perhaps optimistic) SAR-to-alert ratio of 5 percent, this suggests that the industry as a whole is generating and reviewing more than 30,000,000 alerts, presenting a ripe target for efficiency gains. The inefficiency of monitoring systems, not to mention the associated costs, continues to raise concerns in the industry. The financial services regulators, for their part, continue to question the efficacy of transaction monitoring systems that produce such poor results. Both the industry and the regulators often look to different technologies as the solution to the problem.

Protiviti Director Chetan Shah contends that, while the gap between the investment in anti-money laundering (AML) technology and its output remains large, the fault often does not lie with the technology, but with the decisions made to select one system over another, the initial implementation and calibration of the system, and the processes and procedures in place for the ongoing tuning and validation of the system. While the review of transaction activity relies heavily on art – the interpretation of the activity by a skilled reviewer – the effective functioning of a transaction monitoring system depends on science.

Shah answers some questions that can help financial institutions get more out of their transaction monitoring systems.
Q: What are some of the common problems you see in the selection of transaction monitoring systems?

A: Often, we see financial institutions rushing to a decision or being unduly influenced by what systems other companies are using without doing all of the advance work that is necessary. Some of the common gaps we see are:

- The needs assessment is lacking or does not clearly state the functional requirements desired by the institution.
- The project team responsible for developing business and technology requirements and evaluating vendors for technology solutions is not staffed with personnel with relevant business, technical and compliance experience – all three of these disciplines are required.
- There is no methodology, or only one that is poorly defined, to evaluate the solution that best fits with the institution’s business and technology requirements, and overreliance is placed on the following myths:
  - The size of the institution and not its characteristics (e.g., types of customers, products, services, geographies) is the main consideration in selecting a system; the larger the company is, the more expensive and feature-rich the technology should be.
  - Out-of-the-box detection models are sufficient, and no customization or calibration is needed.
  - The solution will overcome any data issues that the company has.
  - The project team takes the high-level, enterprise view and fails to consider the need to customize the solution to address unique needs of different businesses or entities (e.g., inability to monitor products offered by all the divisions or branches of the institution, inability to adjust rules and parameters for different locations, inability to address local privacy laws).
- A cost-benefit analysis is not performed when selecting a new solution or considering upgrades.
- The project team relies too heavily on what the vendor tells them and does not take the time to meet with representatives of other financial institutions that have implemented the solutions being considered to get a “real world” view of the installation process and ongoing use of the tool.

Q: What are the keys to the successful implementation of a transaction monitoring system?

A: Getting the rules/scenarios right begins with understanding the full functionality of the system. Often, we hear from a financial institution that it is manually monitoring certain products because the “system can’t do it,” when the reality is that the financial institution just really doesn’t understand all of the capabilities of the system. Once it is clear which products and transaction types can be accommodated by the system, the next step is to craft the actual rules and scenarios. That is a four-part process that involves a red flag analysis, data acquisition, mathematical analysis to determine the right thresholds at which rules should be executed (here’s where the science starts coming in), and testing. In the red flag analysis, known money laundering typologies (referred to as “red flags”) are mapped to the institution’s products and transaction types to determine whether an automated rule can be used to identify the red flag activity.

When the rules/scenarios have been determined, it is time to consider what data is necessary and where it will be sourced. This step involves identification of various source systems that house the required data. It also involves determining processes that will be responsible for extraction and loading of the data into the
chosen monitoring system. This step requires answering the following questions:

- **Data Availability:** Is the in-scope data readily available?

- **Data Quality:** Has the accuracy of the data been verified? This is a critical step, as inaccurate information (i.e., miscoded transactions) can lead to skewed data analysis and undesired/inaccurate results. As an example, for scenarios designed to capture wires flowing to and from high-risk jurisdictions, it is imperative that the data elements containing the countries through which the wire was routed are present, and that country codes/values are accurate.

- **Data Refresh Rate:** How often is the data refreshed?

- **Data Volume:** Has data analysis been performed to determine data volume? The data volume should be supportable by existing hardware infrastructure either “as-is” or additional hardware resources should be procured.

Once the appropriate rules/scenarios are elected, thresholds need to be determined. Threshold-setting involves calibrating the selected rules/scenarios to execute at an appropriate level for the financial institution. For example, in the case of an aggregation rule, where a customer's entire transaction activity is aggregated on a monthly basis and an alert is generated if the customer's transaction activity exceeds a predetermined value, the focus of threshold-setting would be to identify the aggregated transaction value beyond which the customer's transaction may be considered potentially suspicious. A key point to note here is that even though the same rule (aggregation, in the above example) may be deployed at other financial institutions, the value at which this rule operates at any individual institution will be different, primarily because the type of customers, number of customers and so on will vary from one institution to another. Additionally, the threshold value setting should be influenced by the risk level of the customer. Using the same threshold value for a low-risk customer vs. a high-risk customer can result both in unproductive alerts and missed opportunities to identify potentially suspicious activity.

After completing the above steps and before going into production, a thorough testing of the entire transaction monitoring system is required by the business owners of the system to uncover any design defects that can potentially have a negative impact on the system's overall performance. This step involves creation of test scripts by reviewing the business specifications, creation of a testing environment that has a representative data set identical to production data, execution of the testing scripts and collection of testing results to determine whether the system should be given a go-ahead for production deployment. If material defects are identified, then an additional/multiple beta testing cycle may be required before a go-ahead can be given for production deployment.

It is critical that all of the work done in each of the four steps described above should be documented to provide the information necessary for maintaining and improving the performance of the system and to evidence to regulators and auditors that the configuration of the system was thoughtfully and carefully executed.

Q: What steps can a financial institution take to ensure ongoing effectiveness and even improve the efficiency of a transaction monitoring system?

A: Performing periodic tuning and validation are the best ways to ensure effectiveness and improve performance.

Q: How is tuning performed, and why is it important?

A: Since customer transaction activity is dynamic over time and the volume of customer activity increases as financial institutions grow, it is imperative to perform ongoing tuning to determine
whether the threshold values are still relevant or if they need to be recalibrated, and that the system is still effective and not generating too many false positives. At a high level, the following steps are executed as part of a typical tuning exercise:

• **Quantitative Tuning:** In this phase, a new set of threshold values is determined by performing data mining and advanced statistical analysis on a historical transaction data set. Typically, six to 12 months of transaction data is used, and the most commonly applied techniques are distribution analysis and cluster analysis.

• **Qualitative Tuning:** In this phase, a thorough investigation of sampled alerts generated in the prior step is performed. Key considerations in this step are determining the ratio of good versus bad alerts, operational impacts (alert volumes and staffing levels) and, most important, whether any existing SARs were missed due to the adjustment of existing thresholds.

**Q:** Are there metrics that should be monitored between formal tuning exercises to provide information on the overall performance of a transaction monitoring system?

**A:** The following, which is by no means a complete listing, are some of the metrics that are useful for monitoring the performance of a transaction monitoring system:

• **Number of Alerts Produced by Scenario:** This may alert a financial institution to data issues, such as the possibility that a data feed has been dropped or duplicate transactions are being sourced.

• **Conversion of Alerts to Cases to SARs by Scenario:** This will tell a financial institution how productive each of its scenarios is.

• **Number of SARs Filed That Did Not Originate From an Automated Alert:** This may identify the need to add additional rules/scenarios to the automated system.

• **Alert Patterns:** This will tell whether a scenario is redundant. If there is a very high correlation between the types of scenarios triggering alerts for the same customer, then it may be an indication that the institution is using redundant scenarios.

**Q:** How is validation different from tuning?

**A:** System validation is an exercise in which the entire transaction monitoring system is reviewed by an independent team (e.g., internal audit, a model validation team independent of anti-money laundering [AML] compliance or a qualified third-party firm) to ascertain whether the system is still functioning as designed. This exercise is typically performed on a periodic basis, beginning a year after the system was initially deployed in production because some history is required for the validation exercise to be meaningful. At a high level, the following points are confirmed in a typical validation exercise, which aligns with the expectations of the joint regulatory guidance issued by the Office of the Comptroller of the Currency (OCC) (OCC 2011-12) and the Financial Stability Board (FSB) (SR 11-7).

• **Red Flag Coverage:** In this step, a qualitative review of scenario logic is performed to ascertain whether the system is still providing the appropriate level of coverage.

• **Logic Validation:** In this step, the logic of the scenarios is independently recreated by writing software scripts, executing the scripts against baseline transaction data to generate alerts and reconciling the generated alerts against the alerts in production for the same time period.

• **Threshold Values Validation:** In this step, advanced statistical and data mining techniques are used to determine the threshold values at which each scenario should operate. At a high level, techniques such as distribution analysis, cluster analysis and so forth are leveraged to determine appropriate threshold values.

• **Model Governance:** In this step, the disaster recovery, change control and production support procedures are reviewed for appropriateness.
About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Named one of the 2015 Fortune 100 Best Companies to Work For®, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About Our Risk and Compliance Practice

We partner with management, board members and outside counsel to help organizations comply with regulatory requirements, respond to situations of noncompliance, and improve the processes around information systems supporting governance, risk and compliance (GRC). We help clients take a disciplined approach to managing credit, market and operational risks through a combination of assessments, process improvement, and model review and validation.

At Protiviti, we understand the challenges faced by financial services companies. Our solutions are designed to help your company turn these challenges into competitive advantages.

Contacts

Carol Beaumier  
Managing Director  
+1.212.603.8337  
carol.beaumier@protiviti.com

Cory Gunderson  
Managing Director  
+1.212.708.6313  
cory.gunderson@protiviti.com

Michael Brauneis  
Managing Director  
+1.312.476.6327  
michael.brauneis@protiviti.com

Timothy Long  
Managing Director  
+1.212.399.8637  
timothy.long@protiviti.com

Acknowledgements

Contributors to this newsletter include Steven M. Stachowicz and Chetan Shah.
<table>
<thead>
<tr>
<th>ASIA-PACIFIC</th>
<th>THE AMERICAS</th>
<th>EUROPE/MIDDLE EAST/AFRICA</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUSTRALIA</td>
<td>UNITED STATES</td>
<td>FRANCE</td>
</tr>
<tr>
<td>Brisbane</td>
<td>Alexandria</td>
<td>Paris</td>
</tr>
<tr>
<td>Canberra</td>
<td>Atlanta</td>
<td>Munich</td>
</tr>
<tr>
<td>Melbourne</td>
<td>Baltimore</td>
<td>Frankfurt</td>
</tr>
<tr>
<td>Sydney</td>
<td>Boston</td>
<td>Frankfurt</td>
</tr>
<tr>
<td></td>
<td>Charlotte</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chicago</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cincinnati</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cleveland</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dallas</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Denver</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fort Lauderdale</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Houston</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHINA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Beijing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hong Kong</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shanghai</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shenzhen</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INDIA*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bangalore</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hyderabad</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mumbai</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Delhi</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JAPAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Osaka</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tokyo</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SINGAPORE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Singapore</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Protiviti Member Firm