Fraud governance: It’s more than just compliance

Fraud incidents have increased by over 130% in the past year, resulting in significant monetary and reputational losses for financial institutions. Many of these incidents — including high-profile crimes such as the Society for Worldwide Interbank Financial Telecommunication (“SWIFT”) attacks from last year — involved the exploitation of governance deficiencies and ineffective operating models.¹

Maintaining proper governance for risk management has been a major point of focus for industry groups and regulators, including the Office of the Comptroller of the Currency, the Basel Committee on Banking Supervision, the Committee of Sponsoring Organizations of the Treadway Commission, and the FFIEC.² Accordingly, regulators expect that financial institutions develop an operating model assigning clear roles and responsibilities for risk management — including fraud risk management — across the “three lines of defense.”³

However, the need to develop strong fraud governance practices goes beyond regulatory compliance — such practices are necessary to properly identify and defend against emerging threats that are growing in complexity, including risks related to the Cloud⁴ and digital transformation (e.g., mobile applications), theft of personally identifiable information through business e-mail compromise, and account takeover through mobile self-servicing.⁵ In addition, such practices help organizations operate more efficiently and reduce costs as they result in clear accountabilities, enhanced cross-collaboration, and fraud loss reduction.

To realize these benefits, financial institutions should take steps to establish a strong foundation for fraud risk management, including formalizing governance structures and documenting roles and responsibilities for functional groups. Taking such steps will pave the way for financial institutions to implement a robust three lines of defense operating model for fraud risk management.

This Financial crimes observer discusses key fraud governance challenges, and explains what financial institutions should be doing now.
Key challenges

The most significant challenge we see in achieving a sound fraud management operating model stems from functional silos for fraud prevention and detection. Financial institutions often struggle with clearly defining roles and responsibilities for fraud prevention and detection functions, and ensuring that all three lines of defense are working together effectively and not duplicating roles. As a result, we often see inefficiencies in organizations as activities are unnecessarily duplicated across multiple layers (and lines of defense).

Finally, financial institutions are challenged with navigating the vast and constantly evolving universe of fraud risks. This is especially challenging for larger organizations that have multiple business units, products, and services. As an example, larger organizations that have not dedicated enough resources to fully assess their fraud risks tend to focus their efforts on highly publicized external fraud risks such as business email compromise and account takeover, and often miss key threats facing their organization.

What should financial institutions be doing?

To ensure effective collaboration and coordination across the organization, financial institutions should establish a fraud management operating model using the three lines of defense framework. This framework minimizes the duplications or conflicts that exist between the pursuit of business objectives (first line of defense) and the need for objective risk oversight (second line of defense), while independently assuring that fraud management activities are being carried out in accordance with written policies and procedures (third line of defense).

In establishing this operating model, organizations should develop formal and open communication mechanisms among and within lines of defense teams to enhance information sharing, escalation processes, and prevention capabilities.

Preliminary steps

Prior to implementing a three lines of defense framework, financial institutions should take steps to establish a foundation to support this operating model. These steps include:

- Formalizing governance structures and fraud-focused committees, aligned with broader fraud risk management (e.g., cybersecurity, anti-money laundering, and anti-bribery and corruption) and operational risk management, to oversee and make decisions about fraud.

- Evaluating the target operating model design based on organizational culture and determining whether a centralized, hub-and-spoke, or combination model best suits the organization.

- Developing a RACI (Responsible, Accountable, Consulted, and Informed) model to define expected roles and responsibilities as well as levels of participation for functional groups.

- Documenting roles and responsibilities for each functional group to ensure that duties are properly segregated and critical fraud management activities (e.g., deterrence, prevention and detection, investigation and response, and analytics and reporting) are appropriately addressed.

- Defining reporting lines and requisite skillsets for key fraud risk management roles.

Establishing a “three lines of defense” operating model

Fraud risk management practices should be incorporated throughout each line of defense – business units, independent risk management, and internal audit. Developing this operating model requires clearly defining roles and responsibilities for each line of defense and the functions within them.

First Line of Defense

The first line of defense – the client-facing business – “owns” and manages fraud risk, and drives the building out and bolstering up of fraud risk defenses. Key first line activities include developing and implementing the authentication and fraud strategy, as well as owning the fraud detection, surveillance and analytics, fraud call center, claims management, fraud investigation, recovery, Suspicious Activity Report filing, and business transformation functions.

We recommend that financial institutions formally assign a senior executive from the first line of defense to focus, coordinate, and prioritize fraud prevention and detection efforts on an enterprise-wide basis. This position should be given the autonomy to execute policy and set the tone at the top. Importantly, this fraud management leader is responsible for collaborating closely with the various businesses and product lines (including second line of defense counterparts) to lead the organization to the desired fraud management state.
For example, designing a risk-based authentication strategy involves balancing security concerns with the customer experience. Achieving this balance requires close collaboration between the first line fraud operations, client-facing functions, and information security. Additionally, collaboration between the first line and technology functions is essential to building out the infrastructure needed to detect emerging threats and develop surveillance scenarios. The front line is also responsible for collaborating across the broader financial crimes unit – e.g., with cybersecurity and anti-money laundering functions – to share data and conduct investigations.

Finally, the first line of defense should operate within the guidelines set forth by the second line of defense and follow the frameworks put at their disposal by the second line (as explained below).

**Second Line of Defense**

The primary role of the second line of defense is to provide objective review and credible challenge to fraud risk management efforts carried out by the first line of defense. Accordingly, the second line of defense creates guidelines through which the first line of defense must manage the fraud risks arising from business pursuits — a key component of which is the development of a fraud risk policy (i.e., the written set of standards for fraud risk management) and its companion fraud risk management framework (i.e., the actions that should be taken to meet those standards). The fraud risk management framework includes determining the organization’s fraud risk appetite and developing the fraud risk assessment methodology, fraud model risk management, fraud policy compliance testing requirements, and fraud risk reporting requirements.

One of the biggest challenges faced by the second line of defense is the responsibility to understand the fraud threat landscape and develop a fraud taxonomy – i.e., a classification system designed to assist with the evaluation, organization, and grouping of fraud threats. Taxonomies serve as an essential organizing tool for the analysis and reporting of fraud risk, breaking down threats into their elements, such as actors, method, channel (e.g., online, phone), exposure, and motives. By developing this common language used for reporting and identifying threats throughout the organization, the second line can identify key risk areas and prioritize areas that require additional investment.

Additionally, second line of defense teams provide credible challenge to the first line’s self-assessments to determine risk levels more objectively.

Finally, the second line of defense is responsible for monitoring and testing compliance with fraud policies.

In doing so, the compliance department plays an operational role within the second line of defense. The compliance department is tasked with determining whether the organization is complying with applicable fraud regulations and internal policy as well as determining the activities to be undertaken in order to achieve and maintain compliance with applicable requirements as they evolve.

**Third Line of Defense**

The third line of defense, internal audit, is responsible for providing assurance by independently assessing the design and effectiveness of fraud risk and control policies, frameworks, processes and systems. Accordingly, the main role of the third line of defense in a fraud management operating model is to evaluate the efforts of both the first and second lines of defense.

We have seen a number of financial institutions actively integrate the third line of defense into their fraud management operating model and increase the number of fraud-focused audits, ultimately augmenting the levels of resources dedicated to areas most prone to fraud risk such as client authentication and payment processing.

Additionally, increased regulatory focus on governance and operating models calls for the third line of defense to put more focus on testing fraud prevention and detection capabilities. As a result, financial institutions should determine whether additional investment into their audit departments is necessary to provide an appropriate level of assurance.

**What’s next?**

Financial institutions have made progress in implementing a fraud management three lines of defense operating model, but many still have work to do. Particularly, we have seen the OCC issue “matters requiring attention” (MRAs) regarding first line monitoring of risk activities consistent with risk appetite, the ability of the second line to influence and credibly challenge first line decisions, and the ability of both the first and second lines to proactively mitigate problems.

We expect that regulatory scrutiny of operating models will continue to increase. Because of this regulatory pressure – in addition to the rapidly evolving threat landscape – financial institutions should begin implementing or enhancing their three lines of defense operating model now.
Endnotes

1. For additional information on the SWIFT attacks, see PwC’s Financial crimes observer, SWIFT action: Preventing the next $100 million bank robbery (June 2016).

2. The Federal Financial Institutions Examination Council (FFIEC) is a regulatory council composed of the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Consumer Financial Protection Bureau, and the National Credit Union Administration.

3. Under this framework, the first line of defense, as the business unit, is responsible for owning and managing fraud risks; the second line, consisting of independent risk management functions, is responsible for overseeing and monitoring fraud risks; and the third line, internal audit, provides independent assurance for fraud management activities. For additional information, see PwC’s A closer look, Sales practices: OCC exams and beyond (October 2016).

4. For additional information on the Cloud, see PwC’s financial services digital publication, Get your head in the cloud (August 2016).

5. For additional information on business e-mail compromise and account takeover, see PwC’s Financial crimes observer, Fraud: Email compromise on the rise (February 2016).

6. For additional information, see PwC’s Financial crimes observer, Bank fraud: Old defenses won’t stop new threats (April 2016).

7. The RACI model is a tool for determining roles and responsibilities. It identifies which staff own specific responsibilities, to whom such staff are accountable, which staff can provide support, and which staff must be notified of results.
Additional information

For additional information about this financial crimes observer or PwC’s Financial Crimes Unit, please contact:

Julien Courbe
Financial Services Advisory Leader
646 471 4771
julien.courbe@pwc.com
@JulienCourbe

Jeff Lavine
Financial Crimes Unit Chief Operating Officer
703 918 1379
jeff.lavine@us.pwc.com

Brian Castelli
Anti-Fraud Leader
646 471 2563
brian.castelli@pwc.com

Sean Joyce
Financial Crimes Unit Leader
703 918 3528
sean.joyce@pwc.com
@RealSeanJoyce

Genevieve Gimbert
Anti-Fraud Leader
646 471 5145
genevieve.d.gimbert@pwc.com
@GenGimbert

Roberto Rodriguez
Financial Services Advisory Manager
646 471 2604
roberto.j.rodriguez@pwc.com

Contributing authors: Kristen Gaebel, Astrid Yee-Sobraques, and Kelsey Nencheck.

Follow us on Twitter @PwC_US_FinSrvcs

© 2017 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. PwC US helps organizations and individuals create the value they’re looking for. We’re a member of the PwC network of firms in 157 countries with more than 223,000 people. We’re committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com/us