THE OCC'S FRAUD RISK MANAGEMENT PRINCIPLES

Practical Tips for Implementation

BY JEFF INGBER

In July 2019, the Office of the Comptroller of the Currency issued a bulletin to inform OCC-supervised banks, which include the largest banks in the country, of its conception of sound fraud risk management principles. The pronouncement reinforces previously issued corporate governance and risk management principles and articulates a compendium of existing best practices. It also may be said to reflect many of the basic principles set forth in the long-standing COSO fraud risk management guide. Appendix A to the bulletin contains a long list of OCC, FFEIC and other resources that should be reviewed when developing a comprehensive fraud program. One unlisted item is the Justice Department's "Evaluation of Corporate Compliance Programs," critical guidance for risk management professionals that was updated in April 2019. The DOJ advice overlaps with the OCC's guidance (e.g., referencing metrics, controls, governance, and culture) and can be built on to strengthen it.

The wide range of actions expected is striking – they include training, consumer education, complaint resolution, information security, real-time transaction analysis and behavioral analytics, third-party risk management, and human resources matters such as job breaks and background investigations for new employees. The OCC announcement makes clear the overlap with Bank Secrecy Act measures such as information requests under section 314 of the USA PATRIOT Act (and reinforces the logic of seeking synergies between AML and anti-fraud functions). It also provides that there is no one-size-fits-all approach that is appropriate, as regulatory expectations are derived from the size and complexity of the institution.

With all this in mind, imagine yourself as a risk manager tasked by a bank's senior management with ensuring adherence to all these principles and integrating them into existing anti-fraud policies and processes. The mission is potentially overwhelming. Below are several practical measures that can help.

Ingber.indd 42-43 12/11/19 9:41 AM

1.

Integration of governance/ cross-functional governing board

As the OCC makes clear, proper governance is of paramount importance to controlling a bank's exposure to fraud. But even with a proactive board of directors and senior management engagement, it's still quite challenging to ensure implementation of organization-wide anti-fraud measures. That's because of the breadth of the OCC's principles combined with the stark fact that banks are complex, ever-changing organizations with a range of daily stresses that extend well beyond fraud.

As a practical matter, fraud risk management can't be owned by any one department. Regulators often cite the importance of having each of the three "lines of defense" – the business, the independent risk and compliance functions, and Internal Audit – address key risk issues. What's also critical is unifying ownership organizationally across those three lines and focusing responsibility and oversight. A financial institution might have dozens of committees, subcommittees, and oversight boards that in some manner touch upon fraud. This creates the need for a dedicated anti-fraud committee or council comprised of senior representatives from key business areas, plus functions such as IT, Finance, Compliance, Risk, Vendor Management, HR, and Audit.

A bank's fraud risk management committee should have assigned to it specific key responsibilities that include defining fraud risk appetite and tolerance appropriate to each business line, reviewing anti-fraud policies and procedures, addressing relevant regulatory findings, ensuring a strong anti-fraud control infrastructure, and establishing and taking advantage of MIS systems for identifying and reporting fraud risks and deficiencies. (There may also be a complementary "first line" anti-fraud committee with ongoing test and control responsibilities.) The committee needs to have the resources, stature, and authority appropriate to discharge its responsibilities, including ready access to the bank's senior Risk and Audit Committees to be able to report significant findings together with management's responses and follow-ups.

THE NEED FOR STRONG CULTURE SHOULD BE INTUITIVE, AS FRAUD MITIGATION ULTIMATELY IS ADDRESSED BY PEOPLE, NOT SYSTEMS, AND ALL STAFF MUST UNDERSTAND FRAUD RISKS AND CONTROLS AND VIEW THEM AS REQUIRING ACTIVE SUPERVISION.

2.

Culture

As emphasized by the OCC, a foundation for proper governance is instilling a strong corporate culture that promotes ethical behavior and appropriate tone at the top. "Culture" is a concept that is sometimes neglected because it's hard to define, measure, or quantify. But the need for strong culture should be intuitive, as fraud mitigation ultimately is addressed by people, not systems, and all staff must understand fraud risks and controls and view them as requiring active supervision.

Of course, setting a proper culture begins with a clear commitment from the board of directors and senior management ("tone at the top"). Employees who view their managers as honest, ethical, respectful, and fair are more inclined to emulate that behavior. A positive working environment also will help avoid perceived wrongs that can be the motivation for fraud.

Other important measures to fostering an anti-fraud culture include mandatory employee fraud awareness training, establishing an easily used and understood whistle-blowing process, setting up an effective fraud hotline, disseminating a clear written code of practice covering issues such as the acceptance of gifts, and consistently implementing disciplinary processes for violation of anti-fraud policies.

3.

Control Matrix

The OCC's list of expected detective and preventive controls is wide-ranging and exhaustive. How will implementation of each of the controls be tracked, much less assured? A useful step is to meticulously map them out, including which persons and areas are responsible for specific tasks.

Most financial institutions plot on a heat map the likelihood and significance of various types of fraud, including "Black Swan" events, as well as ordinary risks such as mortgage fraud, insider trading, and identity theft. For regulatory compliance purposes, what's needed as a complement to this is a matrix that documents a bank's fraud risks matched against attendant controls. This should be done for each business process and then aggregated to create the basis for an overall risk appetite statement for fraud.

A potentially useful template to consider as a beginning point is the risk assessment management tool developed by the Association of Certified Fraud Examiners. It includes a matrix showing the identification and evaluation of existing control activities related to each fraud risk exposure and allows for recording the bank's response plan for each. In addition, the template contains pages to record allegations of suspected fraud, investigations and outcomes, and monitoring plans. There are separate columns for identified fraud risks and schemes, a rating of their likelihood and significance, the people and departments responsible, existing anti-fraud controls and whether they are preventive or detective, and an assessment of the effectiveness of the controls, residual risks, and fraud risk response. Again, the ACFE tool is just a start, and will need to be built out to be sufficiently comprehensive.

4.

Metrics and scorecard

The OCC's principles cannot be implemented or demonstrated without the availability of a common view on issues, controls, and residual risk that is accessible and able to be monitored. A monthly fraud risk scorecard can be a useful tool in this regard. The key is to identify a dozen or so critical metrics that quantify actual risk against established risk limits and thresholds. Examples include loss amounts, detection and recovery rates, false positives, call response times, and complaints. These help you best manage fraud while keeping customer impact low.

Attendant to identifying key metrics is determining what constitutes good, average, and poor performance for each metric and assigning a positive or negative point value based on importance. Periodically, you weight each metric based on range, sum up the scores, and evaluate that score.

ON PREVIOUS PAGE: SHUTTERSTOCK.COM

5.

Independent audit and review

The first line of defense is, of course, critical to fraud risk management through measures such as regular testing of controls, analysis of complaint and whistle blower data, and root cause analysis on identified fraud. The second and third lines of defense also are important to ensuring a sound fraud risk management infrastructure, including evaluating processes, vulnerabilities, exposures, and the effectiveness and design of controls. A part of this is analyzing data and assessing where fraud risk is highest, and then auditing or reviewing the OCC-recommended controls in that area. Where fraud has occurred, they should review specifically how the detective and preventative controls failed, and identify opportunities for improvement. These functions also should continuously consider the probability of further errors, fraud, or noncompliance across the organization.

Audits are not the most effective way to uncover fraud, as most frauds are discovered as a result of a tips as well as employee and system detection. Nor can Internal Audit or Independent Compliance and Risk staffers be expected to have the expertise of a person whose primary responsibility is to study fraud. As noted by the Institute of Internal Auditors: "Fraud investigations are best carried out by those experienced to undertake such assignments."

*

Regarding the OCC's important new summary statement of fraud risk management principles, the bottom line is that a cookie-cutter, siloed approach will not suffice. These principles need to be weaved into the bank's organizational structure in a manner such that all who need to contribute can do so, are motivated to do so, are held accountable for doing so, and have their efforts evaluated, measured, reported out, and coordinated logically with all other contributors. ®

JEFF INGBER is chief advisor to the anti-financial crime business at Genpact. He can be reached at jingber@gmail.com.
Jeff thanks Paul Dunlop, Gene Jacobi, and Jennifer Silvestrov Guarini for their thoughtful contributions to this article.

Ingber.indd 44-45 12/11/19 9:41 AM