P&G Banking ADVISOR

Spring 2015

Time for your bank to adopt the updated COSO framework?

Business lending
Taking a savvy spin on due diligence

BANK *Wire*

Cybersecurity preparedness
Be sure to ask the right questions

P&G Associates

www.pandgassociates.com 877.651.1700

Cybersecurity preparedness

Be sure to ask the right questions

Banks today are "critically dependent on IT to conduct business operations," notes the Federal Financial Institutions Examination Council (FFIEC). Given their level of exposure to hackers and other cyber threats, it's more important than ever before for banks' boards and senior management to understand and manage cybersecurity risks.

Last summer, in an effort to evaluate financial institutions' cybersecurity preparedness, the FFIEC piloted a cybersecurity examination work program (the "Cybersecurity Assessment") at more than 500 community banks. Ultimately, the FFIEC will use what it learned to update its guidance to align with changing risks. But the agency's "Cybersecurity Assessment General Observations" helps point banks in the right direction and provides questions for boards and management to consider as they assess their institutions' preparedness. (At ffiec.gov, click on "Cybersecurity Awareness" in the right-hand column to reach the link to the Observations.)

Is your bank well connected?

Inherent cybersecurity risk varies significantly across institutions, the FFIEC stresses. So your bank's first step in evaluating its risk should be to examine its IT activities, including connection types, products and services, and technologies used.

Your bank's first step in evaluating its risk should be to examine its IT activities, including connection types, products and services, and technologies used.

Connection types include virtual private networks (VPNs), wireless networks, local area networks, file transfer protocol (FTP) and bring-your-own-device (BYOD) programs. Because each connection represents a potential entry point for cyber attacks, ask whether your bank really needs all of these connections and whether reducing the types or frequency of connections would improve your management of risk. For example, the risks associated with allowing employees to connect their own devices to the bank's network may greatly outweigh the benefits.

You also should evaluate specialized cybersecurity risks associated with your bank's products and services, such as Automated Clearing House (ACH) and wire transfer services. Criminals could possibly use stolen customer or employee credentials to commit wire transfer or ACH fraud.

ATMs may expose your bank to ATM cash-out scams, and Web-based services may be vulnerable to distributed denial-of-service attacks. Evaluate as well other technologies your bank uses, such as cloud computing and mobile applications. (Also see "Mobile banking apps: Know the risks" on page 3.)

Are you prepared?

Once you have assessed your bank's inherent risks, review your current cybersecurity practices and overall preparedness to mitigate them. The FFIEC urges banks to focus on five areas:

1. Risk management and oversight. Set the "tone at the top" and build a security culture by routinely discussing cybersecurity issues in board and senior management meetings. Ask how accountability for managing cyber risks is determined and about the process for ensuring employee awareness of, and effective response to, cyber risks.

2. Threat intelligence and collaboration. How does your bank gather and analyze threat and vulnerability information? And how does it leverage this information to improve risk management practices? What reports on cyber events and trends does your board receive?

3. Cybersecurity controls. What's your bank's process for devising and implementing preventive, detective, and corrective controls on its network? Do you review and update controls when your IT environment changes? Make sure that you have a process for classifying data and determining appropriate risk-based controls, and for ensuring that identified risks are remediated.

4. External dependency management. Most banks' networks are connected to third parties, such as service providers, business partners and customers. How is your institution connected to these third parties? Identify what your bank is doing to ensure that they're managing their cybersecurity controls. And know their action plans in the event of a cyber attack.

5. Cyber incident management and resilience. A bank should have documented procedures for notifying customers, regulators, and law enforcement of a cyber attack that affects personally identifiable customer information. Have you expanded your bank's business continuity and disaster plans to cover cyber incidents? Do you test these plans regularly?

Mobile banking apps: Know the risks

No bank can afford to ignore mobile banking. Many customers now demand the convenience of such services as remote deposits, mobile bill-paying and person-to-person payments — and the ability to perform them at any time and from anywhere on a smartphone or tablet. Mobile banking benefits banks, too, enabling them to expand their geographic reach without adding physical branches.

Before you introduce mobile banking services, though, it's critical to understand and address the security risks. Because smartphones and tablets are more easily lost or stolen than laptop and desktop computers, mobile banking demands security measures above and beyond those commonly used for Internet banking.

For example, mobile banking apps should be configured so that passwords aren't saved on the device. And multifactor authentication — using fingerprints or other biometric methods, for instance — can help prevent thieves from accessing customers' accounts.

Strength in numbers

One of the most powerful strategies banks can employ in their fight against rapidly evolving cyber threats is to collaborate and share information with other institutions. The FFIEC recommends that institutions of all sizes participate in the Financial Services Information Sharing and Analysis Center (fsisac.com), a private-sector nonprofit information-sharing forum. Information sharing improves your bank's ability to identify, respond to, and mitigate cybersecurity threats and incidents. It also gives you access to the latest techniques for identifying vulnerabilities in your systems and enhancing controls. ▲

Time for your bank to adopt the updated COSO framework?

In 2013, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) updated its *Internal Control — Integrated Framework*, originally published in 1992. COSO's framework is used by most public companies — as well as many privately held financial institutions subject to internal control requirements — to assess their internal control over financial reporting.

COSO recommended that organizations transition to the new framework by Dec. 15, 2014, and now considers the old framework to be superseded. Although many banks continue to use the old framework, at some point it will no longer be considered a "suitable, recognized framework" and banks will need to implement a new one. When that will happen isn't clear, so banks should make the transition as soon as feasible.

Certain banks must comply

A bank is required to conduct a management assessment of internal control effectiveness if it's:

- A publicly traded institution subject to Section 404(b) of the Sarbanes-Oxley Act of 2002 (SOX), or
- A privately held institution with more than $500 million in assets subject to the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA).

Banks in the first category and privately held banks with more than $1 billion in assets must have their external auditors attest to and report on management's assessment of internal control. To satisfy these requirements, covered banks must select a suitable, recognized internal control framework — usually, COSO. And that means implementing updated COSO as soon as feasible.

What about privately held banks with less than $500 million in assets? These banks aren't subject to SOX or FDICIA, but the need for updated internal

controls is likely to trickle down to community banks in the form of heightened regulatory expectations.

Changes include internal control principles

COSO's 2013 update generally retains the original five components of internal control from the 1992 framework: control environment, risk assessment, control activities, information and communication, and monitoring. But the 2013 update supplements those components with 17 "principles of effective internal control" as well as 81 detailed "points of focus" to guide organizations in incorporating those principles.

The update reflects significant changes in the business and operating environments over the last two decades. For example, the 2013 framework explicitly discusses the need to consider potential fraud in assessing risk, places greater emphasis on globalization, provides enhanced guidance on the impact of information technology on business processes and reporting, and details an organization's responsibilities with respect to

outsourced service providers. It also extends beyond external financial reporting to include nonfinancial reporting and internal financial reporting.

What's next?

Making the transition can take time, so the sooner you get started the better. Begin by reviewing and evaluating your current internal control policies, procedures and documentation. Map your existing controls to the 17 principles and 81 points of focus outlined in the updated COSO framework and modify your controls to close any gaps in coverage.

Banks that make the switch to COSO 2013 often find that many of these gaps are caused by missing documentation rather than missing controls. ▲

Business lending

Taking a savvy spin on due diligence

When you begin to analyze a potential borrower's loan worthiness, you know better than to skim the surface. Plunge in to see the full situation and truly understand your customer's financial health.

Sharpen your focus

Start the due diligence process as an auditor would. That is, before you open a borrower's financial statements, consider documenting the risks in the borrower's industry, applicable economic conditions, sources of collateral and the borrower's business operations.

This risk assessment identifies what's most relevant and where your greatest exposure lies, what trends you expect in this year's financials, and which bank products the customer might need. Risk assessments save time because you're targeting due diligence on what matters most.

Review financials in context

Now tackle the financial statements, keeping in mind your risk assessment. First evaluate the reliability of the financial information. If it's prepared by an in-house bookkeeper or accountant, consider his or her skill level and whether the statements conform to Generally Accepted Accounting Principles. If statements are CPA-prepared, consider the level of assurance: compilation, review or audit.

Comprehensive statements include a balance sheet, income statement, statement of cash flows and footnote disclosures. Make sure the balance sheet "balances" — that is, assets equal liabilities plus equity. You'd be

surprised how often internally prepared financial statements are out of balance.

Statements that compare two (or more) years of financial performance are ideal. If they're not comparative, pull out last year's statements. Then, note any major swings in assets, liabilities or capital. Better yet, enter the data into a spreadsheet and highlight changes greater than 10% *and* $10,000 (a common materiality rule of thumb accountants use for private firms). You should also highlight changes that failed to meet the trends you identified in your risk assessment. For example, you expected something to change more than 10% but it did not.

Now ask yourself whether these changes make sense based on your preliminary risk assessment. Brainstorm possible explanations *before* asking the borrower. This allows you to apply professional skepticism when you hear borrowers' explanations.

Devise a scorecard

Use your risk assessment to create a scorecard for each borrower. It often helps to discuss your risk assessment with co-workers and to specialize in an industry niche.

It often helps to discuss your risk assessment with co-workers and to specialize in an industry niche.

One ratio that belongs on every scorecard is *profit margin (net income / sales)*. Every lender wants to know whether borrowers are making money. But a profitability analysis shouldn't stop at the top and bottom of the income statement. It's useful to look at individual line items, such as returns, rent, payroll, owners compensation, travel and entertainment, interest and depreciation expense. This data can provide reams of information on your client's financial health.

Other useful metrics include:

Current ratio (current assets / current liabilities). This measures short-term liquidity or whether a company's current assets (including cash, receivables and inventory) are sufficient to cover its current obligations (accrued expenses, payables, current debt maturities). High liquidity provides breathing room in volatile markets.

Total asset turnover (sales / total assets). This efficiency metric tells how many dollars in sales a borrower generates from each dollar invested in assets. Again, more in-depth analysis — for example, receivables aging or inventory turnover — is necessary to better understand potential weaknesses and risks.

Interest coverage ratio (earnings before interest and taxes / interest expense). This calculation provides a snapshot of a company's ability to pay interest charges. The higher a borrower's interest coverage ratio is, the better positioned it is to weather financial storms.

When applying these metrics, compare a company to itself over time and benchmark it against competitors, if possible. If customers' explanations don't make sense, consider recommending that they hire a CPA to perform an agreed-upon-procedures engagement, targeting specific high-risk areas.

Dig deep

As experience has shown, lenders who only view the surface of a borrower's financial condition can easily be misled. Use available tools to perform due diligence thoroughly. ▲

BANK
Wire

FFIEC UPDATES BSA/AML EXAMINATION MANUAL

As regulators become more aggressive in enforcing Bank Secrecy Act / Anti-Money Laundering (BSA/AML) laws and regulations, banks need to have a strong BSA/AML compliance program. As part of that effort, it's critical to review the FFIEC's revised BSA/AML Examination Manual, released in December 2014.

The updated manual clarifies supervisory expectations and incorporates regulatory changes since the manual's 2010 update. One example: For currency transaction reporting (CTR) purposes, multiple transactions totaling more than $10,000 in one business day should be reported if a bank has knowledge that they are by, or on behalf of, the same person.

Under the revised guidance, the presumption is that separately incorporated entities are independent persons. Thus, separately incorporated businesses that share a common owner shouldn't automatically be aggregated for CTR purposes. Rather, banks should determine, based on information obtained in the ordinary course of business, whether multiple businesses that share a common owner are being operated independently.

You can find the revised manual at ffiec.gov. Click on "BSA/AML InfoBase" on the right side of the page. ▲

WHEN ENDING A TROUBLED DEBT RESTRUCTURING IS OK

As the economy improves, many bankers are wondering whether a loan previously classified as a troubled debt restructuring (TDR) can be restructured. In its third-quarter 2014 supplemental Call Report instructions, the FFIEC said regulators "will not object" to discontinuation of TDR status if:

1. The borrower isn't experiencing financial difficulties (supported by a current, well-documented credit evaluation) at the time of the subsequent restructuring,
2. Under the terms of the subsequent restructuring agreement the bank hasn't granted the borrower a concession (including any prior principal forgiveness on a cumulative basis), and
3. The subsequent restructuring includes interest and other market terms that are no less favorable than those the bank would offer for comparable new debt.

The instructions also provide guidance on accounting for modified TDRs with cumulative principal forgiveness.

Classifying a restructured loan as a TDR can have a significant impact on a bank's financial statements because, for example, TDRs must be measured for impairment, which can result in a loss or valuation allowance. Review your TDRs with the new guidance in mind. ▲

CFPB CAUTIONS LENDERS ABOUT "BURDENING" MORTGAGE APPLICANTS

The Consumer Financial Protection Bureau (CFPB) has warned lenders about imposing illegal burdens on mortgage applicants who receive Social Security disability income. Requiring unnecessary documentation from consumers who receive Social Security disability income may raise fair lending risk. For more information, see CFPB Bulletin 2014-03, "Social Security Disability Income Verification." ▲

P&G Associates

P&G Associates ("P&G") has been meeting the specific risk management needs of community banks of all sizes since 1991. As a high quality and affordable alternative to national firms, P&G provides internal audit, regulatory compliance, BSA/AML, information technology and enterprise risk management review services and software. P&G is exclusively dedicated to the banking industry, providing clients with dedicated, focused and hand-held services reflective of a wide range of skills, experience and industry expertise. As a Firm, we have also been proactive in assisting our clients with the designing, implementation and testing of the internal control environment to assist management with the attestation requirement under the Sarbanes-Oxley Act.

P&G's uniqueness is characterized by its experienced staff and partners. Their hands-on involvement on each engagement provides our clients with a wide range of skills, experience and industry expertise. We employ the use of Subject Matter Experts — designated individuals performing audits in their specific field of expertise. The use of such professionals provides a unique value-added approach that is both efficient and productive.

We believe that a significant aspect of our services is our degree of involvement and responsibility to assist management by making suggestions for improvement, keeping them informed of professional developments and by acting as an independent counsel and sounding board on general business matters and new ideas.

We pride ourselves in our ability to provide effective and practical solutions that are commensurate with our clients' needs by emphasizing high-quality personalized service and attention. Our services are truly customized.

For **Solutions** *to your internal audit needs, please contact our service coordinators at (877) 651-1700, or log-on to www.pandgassociates.com to learn more.*

P&G Associates

www.pandgassociates.com

Headquarters:
646 US Highway 18
East Brunswick, NJ 08816

Offices:
New York, NY
Philadelphia, PA
Chicago, IL
Miami, FL