



Four New Risk Management Requirements Bankers Must Know

By Len Filppu

The laws, requirements, regulations and guidelines of the banking industry can shift and change with little notice, sometimes leaving bankers bewildered and unaware of the latest new wrinkles. Unfortunately, ignorance of the latest rules is not an excuse and does not prevent a bank from being written up come examination time. With sound risk management planning and clean regulatory reviews as the goal, the following are four recent requirements to keep in mind.

The New FDIC Information Technology Examination Questionnaire

The FDIC has updated its risk-based information technology examination process for FDIC-supervised banks, and while many banks are under the supervision of OCC, FRB and OTS, these important changes reflect a trend filtering throughout the regulatory industry.

The new IT examination process focuses on a bank's information security program and risk management procedures for securing information. It contains five major sections: Risk Assessment, Operations Security and Risk Management, Audit/Independent Review Program, Disaster Recovery and Business Continuity, and, GLBA/FDIC Rules and Regulations - 122 CFR Part 364 Appendix B.

Most of these sections contain familiar guidelines; however, there is one important new area that may save banks time and money. The Information Technology Risk Assessment guidelines now require an analysis of GLBA-related threats to confidential customer and consumer information. Most banks already perform an annual IT Risk Assessment and a GLBA Risk Assessment. Industry professionals opine that banks should now be able to perform just one annual IT Risk Assessment that will satisfy both the IT risk and GLBA compliance requirements.

Enhanced BSA Examination Guidelines

The FFIEC recently published a uniform examination manual for Bank Secrecy Act/Anti Money Laundering. Going forward, each regulatory agency will be using the same examination program. Differences will depend on the relative money laundering risk at each institution.

The new manual is a substantial 331 pages, and contains extensive background on money laundering risks for various types of bank products, services, customers and geographies. It also contains the work program to be used by the examiners.

The following eight points comprise the majority of the internal audit and risk management expectations. The audit scope should be reviewed with your internal auditor (whether in-house or third party) to ensure these minimum expectations are being met. Additionally, the new manual will serve as an excellent reference tool answering most BSA/AML questions.

- An evaluation of the overall integrity and effectiveness of the BSA/AML compliance program.
- A review of the risk assessment for reasonableness given the bank's risk profile (products, services, customers, and geographic locations).
- Appropriate transaction testing to verify adherence to the BSA recordkeeping and reporting requirements.

- An evaluation of efforts to resolve violations and deficiencies noted in previous audits and examinations.
- A review of staff training for adequacy, accuracy, and completeness.
- A review of the effectiveness of the suspicious activity monitoring systems.
- An assessment of the overall process for identifying and reporting suspicious activity, including a review of completed SARs to determine accuracy, timeliness, completeness, and effectiveness of BSA/AML policy.
- Documentation of audit work including scope, procedures performed, transaction testing completed, and findings. The audit work papers should be available for examiner review. Audit results should be reported directly to the board or a board committee.

Importance of Overall Bank Risk Assessments

Widespread reports are emerging about regulators criticizing banks during safety and soundness examinations for not adequately completing overall bank risk assessments that direct their internal audit programs. Criticism in this area can adversely affect a bank's management score.

The overall bank risk assessment identifies the major services, products and functions of the bank. A "Risk" score is then assigned for each major risk criteria based upon the transaction activity and overall operating environment of the function. The risk factors are based upon activity relative to the overall assets, income and losses of the bank, and then ranked by degree of risk - minimal, low, moderate, high or priority. Based upon this ranking, suggested internal audit program scoping and frequency is recommended. Risk assessments should be performed by someone independent of bank management such as the bank's internal auditor or a third party internal audit provider.

Regulators and audit committees alike appreciate overall bank risk assessments because they demonstrate a systematic, independent and comprehensive approach to risk management while containing costs by focusing on the areas most in need of internal audit attention.

New Focus on Risk Management Vendor Management

Banks already conduct due diligence for vendors who perform outsourced core processing or other operations services. But due diligence is now being examined in the selection of outsourced risk management providers. It's important to remember that using vendors and other third parties does not diminish the responsibility of the bank's directors and management to ensure that all activity is conducted in compliance with applicable laws and in a safe and sound manner.

The following checklist will assist in the hiring of the most responsible risk management vendors, and will also document due diligence to satisfy inquiring regulators.

Risk Management Vendor Selection Checklist

1. Does vendor provide you with proof of liability insurance?
2. Have you checked and documented responses from at least three vendor references?
3. Does vendor provide a financial statement that ensures financial viability?
4. Does vendor retain work papers for seven years (or provide you the work papers for storage/retention at the bank)?

5. Does vendor have sufficient qualified staff to perform all specialized services?
6. For IT audits, does vendor's IT audit staff hold advanced IT certifications such as CISA or CISSP?
7. Does vendor firm have management depth to ensure continuity of services due to personnel changes, illness, etc.?
8. Does vendor provide clear, timely professional reports?
9. Does vendor provide a written contract containing full scoping and a non-disclosure clause?
10. Is vendor an active member in good standing of industry organization and associations?

Len Filppu is executive vice president/director of operations for AuditOne LLC (www.audit-one.com), a San Jose, Calif.-based independent internal audit firm specializing in banks and their service providers throughout the western United States. He can be reached at 408-980-8099 or len.filppu@audit-one.com.

http://www.wib.org/publications_resources/article_library/2005-06/apr06_risk_man.html