



Roadmap for the Maze of Risk Assessments

By Len Filppu

Bank directors today face a higher level of responsibility to ensure their institutions are properly managed, and risk assessments are excellent tools that help bank management cost-effectively invest limited resources in appropriate places. But the variety of risk assessments can be bewildering.

There are four primary risk assessments crucial to a bank's risk management strategy. They are 1) Overall Bank risk assessment; 2) Information Technology risk assessment; 3) Gramm-Leach-Bliley Act (GLBA) risk assessment; and 4) Bank Secrecy Act/Anti Money Laundering (BSA/AML) risk assessment.

Overall Bank Risk Assessment

Regulators are increasingly looking for overall bank risk assessments as the guiding tool to set risk management policy, and they've been known to criticize banks (especially de novo banks) during safety and soundness examinations for not adequately completing overall bank risk assessments. Criticism in this area can adversely affect a bank's management score.

Overall bank risk assessments drive the internal audit strategy, plan and calendar. This 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. Based upon this ranking, an internal audit program and calendar is recommended. Overall bank risk assessments should be performed annually by someone independent of bank management such as the bank's internal auditor or a third party provider.

BSA/AML Risk Assessment

The Federal Financial Institutions Examination Council's (FFIEC) uniform examination manual for BSA/AML requires an annual risk assessment that considers the money laundering risk inherent in a bank's products, services, customers, and geographic locations. No particular format is required, but the BSA/AML risk assessment should be concise and organized, and communicated to the bank's management, Board, business lines, and appropriate staff.

The BSA/AML risk assessment performs a detailed analysis within each category by considering activity risks. The bank must create a Customer Identification Program (CIP), Customer Due Diligence (CDD) procedures, and appropriate BSA/AML controls based upon the risks. The risk assessment must be updated whenever there are significant changes to a risk category, and banks should conduct independent testing of controls annually.

IT Risk Assessment

As technology increasingly permeates all aspects of banking, regulators are emphasizing a risk-based approach to IT examinations. The FFIEC IT Examination Handbook states that banks must maintain an ongoing information security risk assessment program that basically considers:

- all information and technology assets
- threats and vulnerabilities to confidential information for each asset
- the probability and impact associated with the threats and vulnerabilities

- prioritization of the risks
- identification of appropriate controls
- appropriate level of training necessary for mitigation.

Guidelines now also require IT risk assessments to include an analysis of GLBA-related threats to confidential information. The IT risk assessment must be updated whenever new systems and products are placed into production mode. Bank communications channels should be institutionalized to update the risk assessment. The bank's board of directors should receive an annual IT security report that also contains GLBA-related information.

GLBA Risk Assessment

Essentially, GLBA requires banks to design, implement and maintain security safeguards to protect confidential customer information. Under section 501b, the process generally requires banks to perform a GLBA risk assessment, develop an information security policy, and conduct annual testing. Regulators expect banks to perform their own GLBA risk assessments annually. While an independent consulting firm can assist in this process, the GLBA risk assessment final product must ultimately be the bank's responsibility.

Developing a GLBA risk assessment is made manageable and cost-effective by employing a simple matrix. A GLBA risk matrix should first list the bank's major information assets. Then for each asset, list: 1) threat types, such as malicious intent, accidental leakage, external factors, vendor leakage; 2) inherent likelihood and impact of threats; 3) mitigating bank controls; and 4) residual probability and impact.

Two-for-One Strategy: Combining IT and GLBA Risk Assessments

Most banks already perform an annual IT risk assessment and a GLBA risk assessment. Industry professionals opine that banks may now be able to perform one annual risk assessment that will satisfy both the IT risk and GLBA compliance requirements. Bagging two birds with one stone may be a sound and cost-effective strategy.

Final Thought

Risk is acceptable. Banks are evaluated on how they manage risk. It's important to document risk management actions, and the risk assessments discussed are excellent tools for this purpose.

Len Filppu is executive vice president/director of operations for AuditOne LLC in San Jose , Calif. Filppu and AuditOne can be reached at 408-980-8099 or Len.filppu@audit-one.com or www.audit-one.com.

http://www.wib.org/publications_resources/article_library/2005-06/oct06_roadmap.html