BBL The Bank Board Letter

December 2012

Edited exclusively for directors of financial institutions and their holding companies

# Strategic risk: what the board should know and do about it

**BY CATHY GHIGLIERI**

Strategic risk is currently a focus of regulatory scrutiny and the board of directors should understand what it is and how to manage it. Strategic risk is the risk to a bank's earnings and capital from making poor business decisions, from not implementing business decisions properly or from failing to respond to industry changes.

For example, strategic risk is increased when a bank offers a new product or service without having the experienced personnel or the appropriate infrastructure in place first. Strategic risk is also increased when a bank embarks on a new venture without conducting adequate due diligence or without having appropriate risk controls established.

The board of directors can assess the level of strategic risk by reviewing the bank's goals, along with the strategies and implementation plans to meet those goals. The review should include an analysis of the resources available to meet the goals, including the sufficiency of bank's management team, technology, operations and communications.

External factors that might affect successfully meeting the bank's goals should also be analyzed, including changes in the economy, taxes, regulatory environment, competition and technology, just to name a few.

Strategic risk cannot truly be managed, however, unless the board of directors understands the total risks that exist across the entire bank. For example, the board cannot appropriately decide to offer a new lending product without considering the risk levels present in the bank's technology, liquidity and capital adequacy.

Similarly, the board cannot appropriately decide to expand its footprint without considering the risk present in the bank's current level of operations. If the bank does not have sufficient management expertise, or if the bank's operations and technology lack the ability to handle the new business, strategic risk is increased by being unable to properly implement this business decision.

Strategic risk, therefore, is necessarily a component of the broader analysis called enterprise risk management. ERM is the assessment and management of risk across the whole bank or enterprise. If the bank has not yet conducted an ERM assessment, now is the time to begin the process. While there is no one right way to conduct an ERM assessment, the depth and breadth of the review will necessarily depend on such things as the complexity of the bank, the types of products and services it offers, and the technology currently in use.

One place to begin the ERM assessment is to identify and assess risk across the enterprise using the nine categories of risk outlined by the Office of the Comptroller of the Currency, which include the following:

— Credit risk: the risk to earnings and capital from the failure to be repaid on a loan.

— Interest rate risk: the risk to earnings and capital from movements in interest rates.

— Price risk: the risk to earnings and capital from changes in the value of investment portfolios.

— Transaction risk: the risk to earnings and capital from fraud, error or inability to deliver products or services.

— Reputation risk: the risk to earnings and capital from negative public opinion, gossip, rumors or press reports.

— Compliance or legal risk: the risk to earnings and capital from violations of law, regulation, internal policies or ethical standards.

— Strategic risk: the risk to earnings and capital from adverse business decisions.

— Foreign exchange risk: the risk to earnings and capital from the conversion from one currency to another.

— Liquidity risk: the risk to earnings and capital of failing to meet obligations as they come due.

These nine risk categories are intertwined. For example, a growing exposure to interest rate risk could affect credit, price and liquidity risks. Likewise, the potential noncompliance with certain laws and regulations (compliance risk) could affect not only reputation risk, but also liquidity risk.

Conducting an ERM analysis is no small task. But once it is completed, the results may be used in several ways. First, the board of directors should discuss how the current risk levels should be managed or reduced in order to meet the bank's profitability goals. The negative impact to a bank's profits from increasing loan losses or narrowing margins is obvious. But what about the negative impact on profits due to fair lending compliance problems?

Second, the ERM analysis should be factored into the strategic plan. Discussions at the annual strategic planning retreat could address such questions as: Are the present products and services the right ones for the board's risk appetite? Is the level of risk within the tolerances established by the board of directors or should these tolerances be adjusted or the risk reduced? And third, the ERM analysis should be factored into the bank's capital planning in order to more knowledgeably determine how much capital will be needed over the next five years considering all of the risks present in the bank.

Making business decisions without knowing all of the risks present in the bank is a tricky proposition for the board of directors and can increase the level of strategic risk, as well as harm the future profitability of the bank. Performing an enterprise risk management analysis is

time-consuming, but the results can be critical for the board in moving the bank forward in a profitable and sound way.

Utilizing the results of a full enterprise risk management assessment prior to making any major business decisions will improve the bank's strategic risk and will enhance the bank's chances of meeting or exceeding its strategic goals.

Assessing the bank's strategic risk, armed with valuable information from an ERM assessment, will not only bode well for the bank's next examination, but also will assist the board in making sound business decisions in the future.

---

*Cathy Ghiglieri is a former Texas Banking Commissioner and president of Ghiglieri & Co., a bank conculting firm in Austin, Texas. She is the co-autor of* The Ultimate Guide for Bank Directors. *Contact her at www.ghiglieri.com.*

# The sleeper risk of 2012: vendor management

**BY PAUL REYMANN**

Regulators are making third-party compliance a priority. And believe it or not, community banks are liable for the damage caused by improper vendor actions. The Consumer Financial Protection Bureau issued a statement earlier this year that reminded banks they are liable for the actions of the companies they contract with.

"Consumers are at a real disadvantage, because they do not get to choose the service providers they deal with — the financial institution does," said CFPB Director Richard Cordray in the bureau's press release on the guidance. "Consumers must not be hurt by unfair, deceptive or abusive practices of service providers. Banks and nonbanks must manage these relationships carefully and can be held accountable if they break the law."

Yet with the increase in outsourcing activities and the added regulatory attention, community banks have not identified vendor management as a priority. ATTUS Technologies Inc. and its parent, Computer Services Inc., recently surveyed hundreds of financial institutions for their insight on banking priorities for the current year. While the survey covered numerous areas of banking activities, the topic of vendor management was resoundingly silent. Few, if any, respondents recognized it as a priority for 2012.

To effectively manage a bank's vendors, institutions should focus on four key areas: vendor selection, vendor contract, vendor management, and monitoring and contingency planning.

**Vendor Selection**

Conducting proper due diligence in selecting a vendor is a critical aspect of vendor risk management. Important due diligence steps include:

— Asking the vendor to provide references (particularly ones from other financial institutions) to determine satisfaction with the vendor's performance.

— Asking questions about the vendor's data backup system, continuity and contingency plans, and management information systems.

— Researching the background, qualifications and reputations of the vendor's principals.

— Determining how long the vendor has been providing the service.

— Assessing the vendor's reputation, including lawsuits filed against it.

— Obtaining audited financial statements to check the vendor's financial health.

**Vendor Contract**

The contract between the financial institution and the vendor is another key factor in mitigating risk, because it dictates legally binding terms and conditions. Financial institutions should rely on experienced counsel to ensure that its interests are protected and potential contingencies are considered. The contract should also articulate the mutual expectations of both parties.

**Vendor Management and Monitoring**

After the vendor has been selected and the contract signed, it is important to manage and monitor the relationship. Senior management should be involved in approving policies and procedures to monitor the vendor's performance and activities. Performance monitoring controls should include:

— Grouping vendors into criticality categories (i.e., high, medium and low).

— Ensuring that the vendor is complying with consumer protection laws and regulations.

— Periodically analyzing the vendor's financial condition and performing on-site quality assurance reviews.

— Regularly reviewing metrics for the vendor's performance relative to service level agreements.

— Reviewing customer complaints for services or products handled by the vendor and conducting anonymous testing if applicable (mystery shopper).

— Assessing whether contract terms are being met.

— Testing the vendor's business contingency planning.

— Evaluating the vendor's information security practices ensuring the protection of sensitive customer information.

— Evaluating adequacy of the vendor's training to its employees.

— Periodically meeting with the vendor to review contract performance and operational issues.

**Contingency Planning**

While outsourcing can be beneficial, it creates the risk that a vendor's operations can be disrupted and might affect the bank for the services the vendor provides. To mitigate this risk, financial institutions must ensure that the vendor has a prudent business recovery plan in place.

In the end, vendor management is a matter of building in the proper processes before you have an issue with a company. Prepare by building a strong plan for managing, testing and evaluating vendors so that your bank will not be caught off-guard when the next examination rolls around.

---

*Paul Reymann is chief risk officer of Charlotte, N.C.-based ATTUS Technologies Inc., a wholly owned subsidiary of Computer Services Inc. For more information, visit www.attustech.com.*