[BSP CIRCULAR NO. 511, S. OF 2006, February 03, 2006]

GUIDELINES ON TECHNOLOGY RISK MANAGEMENT

The Monetary Board in its Resolution No. 69 dated 19 January 2006, approved the adoption of the attached guidelines on technology risk management to ensure that banks have the knowledge and skills necessary to understand and effectively manage their technology-related risks.

The guidelines contain two main parts. The first outlines the primary risk related to the bank's use of technology and the second describes a risk management process on how banks should manage these risks. Key points include the following:

- The use of technology-related products, services, delivery channels and processes exposes a bank to various risks, particularly Operational, Reputation, Compliance and Strategic risk.

- Banks are expected to have an integral approach to risk management to identify, mea- sure, monitor, and control risks. Technology-related risks should be reviewed together with other bank risks to determine the bank's overall risk profile.

- In using technology, bank management should engage a rigorous analytic process to identify and quantify risks, to the extent possible, and to establish risk controls to manage risk exposures.

- Technology-related risk management process involves three essential elements:

  - Planning
  - Implementing
  - Measuring and Monitoring Performance

  These elements are critical to an effective technology-related risk management process of a well-managed institution, regardless of size.

This Circular shall take effect fifteen (15) days after publication in the Official Gazette or in a newspaper of general circulation.

Adopted: 3 Feb. 2006

(SGD.) AMANDO M. TETANGCO, JR.
Governor

Guidelines on Technology Risk Management

I. Background

Banks using technology-related products, services, delivery channels, and processes can be exposed to all types of risks enumerated under the Bangko Sentral ng Pilipinas risk supervision framework more particularly Operational, Strategic, Reputation, and Compliance risk. With banks' increased reliance on technology, it is important for the banks to understand how specific technologies operate and how their use or failure may expose banks to risk. The Bangko Sentral ng Pilipinas expects banks to have the knowledge and skills necessary to understand and effectively manage their technology-related risks. The Bangko Sentral ng Pilipinas will evaluate technology-related risks in terms of the categories of risks identified in its Risk Assessment System.

II. Description of Technology Related Risks

Operational Risk

This is the risk to earnings or capital arising from problems with service or product delivery. This risk is a function of internal controls, information systems, employee integrity, and operating processes. Operational risks exists in all products and services.

Technology can give rise to operational risk in many ways. Operational risk often results from deficiencies in system design, implementation, or ongoing maintenance of systems or equipment. For example, incompatible internal and external systems and incompatible equipment and software expose a bank to operational risk. Operational risk can increase when a bank hires outside contractors to design products, services, delivery channels, and processes that do not fit with the bank's systems or customer demands. Similarly, when a bank uses vendors to perform core bank functions, such as loan underwriting and credit scoring, and does not have adequate controls in place to monitor the activities of those vendors, operational risk may increase. Also, when banks merge with other banks or acquire new businesses, the bank's combined computer systems may produce inaccurate or incomplete information or otherwise fail to work properly. The failure to establish adequate security measures, contingency plans, testing, and auditing standards also increases operational risk.

Strategic Risk

This is the risk to earnings or capital arising from adverse business decisions or improper implementation of those decisions. This risk is a function of the compatibility of an organization's strategic goals, the business strategies developed

to achieve those goals, the resources deployed against these goals, and the quality of implementation. The resources needed to carry out business strategies are both tangible and intangible. They include communication channels, operating systems, delivery networks, and managerial capacities and capabilities.

Use of technology can create strategic risk when management does not adequately plan for, manage, and monitor the performance of technology-related products, services, processes, and delivery channels. Strategic risk may arise if management fails to understand, support, or use technology that is essential for the bank to complete or if it depends on a technology that is not reliable. In seeking ways to control strategic risk, a bank should consider its overall business environment, including: the knowledge and skills of senior management and technical staff; its existing and planned resources; its ability to understand and support its technologies; the activities and plans of suppliers of technology and their ability to support the technology; and the anticipated life cycle of technology-related products and services.

Reputation Risk

This is the risk to earnings or capital arising from negative public opinion. This affects the institution's ability to establish new relationships or services, or to continue servicing existing relationships. This risk can expose the institution to litigation, financial loss, or damage to its reputation. Reputation risk exposure is present throughout the organization and that is why banks have the responsibility to exercise an abundance of caution in dealing with its customers and community. This risk is present in activities such as asset management and regulatory compliance.

Reputation risk arises whenever technology-based banking products, services, delivery channels, or processes may generate adverse public opinion such that it seriously affects bank's earnings or impairs capital. Examples may include: flawed security systems that significantly compromise customer privacy; inadequate contingency and business resumption plans that affect a bank's ability to maintain or resume operations and to provide customer services following system failures; fraud that fundamentally undermines public trust; and large-scale litigation that exposes a bank to significant liability and results in severe damage to a bank's reputation. Adverse public opinion may create a lasting, negative public image of overall bank operations and thus impair a bank's ability to establish and maintain customer and business relationships.

Compliance Risk

This is the risk to earnings or capital arising from violations of, or non-conformance with laws, rules, regulations, prescribed practices, or ethical standards. Compliance risk also arises in situations where the laws or rules governing certain bank products or activities of the bank's clients may be ambiguous or untested. Compliance risk exposes the institution to fines, civil money penalties, payment of damages, and the voiding of contracts. Compliance risk can lead to a diminished reputation, reduced franchise value, limited business opportunities, lessened expansion potential, and the lack of contract enforceability.

Compliance risk may arise in many different ways. For example, it may arise when a bank fails to comply with applicable disclosure requirements or when it discloses information to outside party that it is required to keep confidential. Compliance risk also may arise when a bank does not have systems in place to ensure compliance

with mandatory reporting statutes. The use of technology to automate lending decisions also could expose a bank to compliance risks if the programs are not properly tested or if the quality of the data is not verified. For example, the use of credit scoring models to automate lending decisions could expose a bank to compliance risk if the data upon which the program rely are flawed or if the program design itself is flawed.

As banks move increasingly from paper to electronic-based transactions and information exchanges, they need to consider how laws designed for paper-based transactions apply to electronic-based transaction and information exchanges. Some new technologies raise unexpected compliance issues. Transactions conducted through the internet also can raise novel questions regarding jurisdictional authority over those transactions. Therefore, banks should be careful to monitor and respond to changes to relevant laws and regulations arising from these developments.

III. Technology Risk Management Process

The technology risk management process is designed to help the bank to identify, measure, monitor, and control its risk exposure. The process involves three essential elements, namely:

a. Planning
b. Implementing
c. Measuring and Monitoring Performance

It is the responsibility of Bank's Board of Directors and a Senior Management Committee to ensure that an effective planning process exists, that technology is implemented properly with appropriate controls, and that measurement and monitoring efforts effectively identify ways to manage risk exposure. The process should be more complex for larger institutions, particularly for those with major technology-related initiatives.

For each IT project, the bank should adopt specific milestones and corresponding timelines up to the full implementation of the IT project.

Planning

Technology planning often involves strategic, business, and project planning.

- Strategic plan establishes the overall role of technology as it relates to the bank's mission and assesses the type of technology that a bank needs to fullfill that role.

- Business plan integrates the new technology into existing lines of business and deter- mines the level of technology best suited to meet the needs of particular business lines.

- Project plan establishes resource needs, time lines, benchmarks, and other information necessary to convert the business plan into operation.

The review and planning cycle may vary depending on the type of institution and its uses of different types of technologies. Proper planning minimizes the likelihood of computer hardware and software systems incompatibilities and failures, and maximizes the likelihood that a bank's technology is flexible enough to adapt to future needs of the bank and its customers.

Because technology is constantly changing, bank management should periodically assess its uses of technology as part of its overall business planning. Such an enterprise-wide and ongoing approach helps to ensure that all major technology projects are consistent with the bank's overall strategic goals. Planning should consider issues such as:

- Cost of designing, developing, testing and operating the systems whether internally or externally;

- Ability to resume organizations swiftly and with all data intact in the event of system failure or unauthorized intrusions;

- Adequacy of internal controls; including controls for third party providers; and

- Ability to determine when a specific risk exposure exceeds the ability of an institution to manage and control that risk.

In cases when specialized expertise is needed to design, implement, and service new technologies, vendors may provide a valuable means to acquire expertise and resources that a bank cannot provide on its own. However, in planning on whether and how to contract for its technology needs, a bank should assess how it will manage the risks associated with these new relationships. Without adequate controls, the use of vendors to design or support new bank technologies and systems could increase a bank's exposure to risk. While a bank can outsource many functions, management remains responsible for the performance and actions of its vendors while the vendors are performing work for the bank.

To have an effective planning process for technology-related applications, bank's planning process should at least have the following basic components:

Involvement of the Board of Directors and Senior Management

The Board of Directors and a Senior Management Committee play an important role in managing bank's IT risks. Both should have knowledge of and involvement in the technology planning process.

The board of directors and the senior management committee should review, approve, and monitor technology projects that may have a significant impact on the bank's operations, earnings or capital. In addition, senior management is expected to have more involvement in and more knowledge about the day to day operations of these projects than the board of directors. At least one key senior manager should have knowledge and skills to evaluate critically the design, operation and oversight of technology projects. The board should be fully informed by the senior management committee, on an ongoing basis, of the risks that technology projects may pose to the bank.