



Bangko Sentral ng Pilipinas

MAYNILA, PILIPINAS

OFFICE OF THE GOVERNOR

Circular No. 511
Series of 2006

Subject: 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 integrated approach to risk management to identify, measure, 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:
 1. Planning
 2. Implementing
 3. 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.

FOR THE MONETARY BOARD:


AMADOR 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 risk 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 compete 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 a 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 fulfill that role.
- Business plan integrates the new technology into existing lines of business and determines 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 operations 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.

Banks that use technology extensively, particularly large banks, should have sufficient expertise and knowledge among managers and staff to provide critical review and oversight of technology projects and to manage risks associated with them. Projects should be coordinated to ensure that they adhere to appropriate policies, standards, and risk management controls. In addition, senior managers with knowledge of the bank's technology initiatives should report periodically to the board of directors on technology-related initiatives.

Gathering and Analysis of Relevant Information

Banks should consider existing systems, consumer expectations, and competitive forces in their planning for new or enhanced uses of technology. In the process of gathering and analyzing information, bank should:

- Inventory existing systems and operations. Bank should review their existing systems to determine whether they satisfy current and projected bank needs. They should also evaluate how new technologies will fit into existing systems and whether additional changes to those systems will be necessary to accommodate the new technologies.

- Review industry standards. Bank management should assess current and developing industry standards in determining whether to implement specific technologies. Technical standards help to ensure that systems are compatible and interoperable.
- Determine when to deploy new technology. Timing is critical because there are risks in deploying new technologies too slowly or too rapidly.

Assessment and Review

Bank management should carefully assess its technology needs and review its options within the context of overall planning. Management should consider whether the necessary resources, time, and project management expertise is available to successfully complete any new technology proposal. Prior to adopting new technologies, bank management should identify weaknesses or deficiencies in the bank's ability to use them. Management should also consider whether staff can operate both new and existing systems simultaneously. These considerations will help management to choose the type and level of technology best suited to support its key business needs and objectives.

Banks should be cautious in establishing project objectives and should ensure that the objectives are neither too ambiguous nor too ambitious. Management should control the bank's risk exposure through practical planning. This planning may include dividing projects into manageable segments and establishing specific decision points as to whether a project should be modified or terminated. Planning should also establish contingency and exit plans in the event a new project does not proceed as planned.

Management should assess and, where possible, attempt to quantify the costs and benefits of adopting new technology when reviewing its options. As part of this assessment, management should evaluate the risks, financial consequences, and likelihood that certain risks may occur. This review should also include assessment of the cost to start, run, and terminate a project.

Implementation

Proper implementation of projects and initiatives is needed to convert plans into better products and services, delivery channels, and processes. Banks should establish the necessary controls to avoid operational failures and unauthorized intrusions which could result in increased losses and damaged reputation. At a minimum, management should establish technology standards that set the direction for the bank in terms of the overall structure or architecture of its technology systems.

Management should establish priorities to ensure proper coordination and integration of projects among managers, work units, and team members. It should provide clearly defined expectations, including user and resource requirements, cost estimates, project benchmarks, and expected deliver dates. Proper project monitoring by all relevant parties is important. Project managers should inform the senior management committee of obstacles as early as possible to ensure that proper controls are in place and corrective action can be taken to manage risk exposure.

Proper project implementation should include the following:

a. Controls

Controls comprises of policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.

Banks should adopt adequate controls based on the degree of exposure and the potential risk of loss arising from the use of technology. Controls should include clear and measurable performance goals, the allocation of specific responsibilities for key project implementation, and independent mechanisms that will both measure risks and minimize excessive risk-taking. These controls should be re-evaluated periodically.

Bank information system security controls are particularly important. Security measures should be clearly defined with measurable performance standards. Responsible personnel should be assigned to ensure a comprehensive security program. Bank management should take necessary steps to protect mission-critical systems from unauthorized intrusions. Systems should be safeguarded, to the extent possible, against risks associated with fraud, negligence, and physical destruction of bank property. Control points should include facilities, personnel, policies and procedures, network controls, system controls, and vendors. For example, security access restrictions, background checks on employees, separation of duties, and audit trails are important precautions to protect system security within the bank and with vendors. As technologies and systems change or mature, security controls may need to change periodically as well.

b. Policies and Procedures

Bank management should adopt and enforce appropriate policies and procedures to manage risk related to bank's use of technology. The effectiveness of these policies and procedures depends greatly on whether they are in practice among bank personnel and vendors. Testing compliance with these policies and procedures often helps banks correct problems before they become serious. Clearly written and frequently communicated policies can establish clear assignments of duties, help employees to coordinate and perform their tasks effectively and consistently, and aid in the training of new employees. Bank management should ensure that policies, procedures, and systems are current and well-documented.

c. Expertise and Training

Bank management should ensure that key employees and vendors have the expertise and skills to perform necessary functions and that they are properly trained. Management should allocate sufficient resources to hire and train employees and to ensure that there is succession planning particularly for the critical officers of the bank. Training may include technical course work, attendance at industry conferences, participation in industry working groups, as well as time allotment for appropriate staff to keep abreast of important technological and market developments. Training also includes customer orientations to ensure that bank's customers understand how to use or access bank's technology products and services and that they are able to do so in an appropriate and sound manner.

d. Testing

Bank management should thoroughly test new technology systems and products. Testing validates that equipment and systems function properly and produce the desired results. As part of the testing process, management should verify whether new technology systems operate effectively with the bank's existing systems and, where appropriate, should include vendors. Pilot programs or prototypes can be helpful in developing new technology applications before they are used on a broad scale. Testing should be conducted periodically to help manage risk exposure.

e. Contingency Planning and Business Resumption Planning

Bank's systems should be designed to reduce bank's vulnerability to system failures, unauthorized intrusions, and other problems. Bank should have back-up systems in place and they should be maintained and tested on a regular basis to make sure that they will be readily available when the need arises. The risk of equipment failure and human error is possible in all systems. This risk may result from sources both within and beyond bank's control. System failures and unauthorized intrusions may result from design defects, insufficient system capacity, and destruction of a facility by natural disasters or fires, security breaches, inadequate staff training, or uncontrolled reliance on vendors.

Bank should have business continuity plans in place before bank implements new technology. They should establish a bank's course of action in the event of a system failure or unauthorized intrusions and should be integrated with all other business continuity plans for bank operations. The plan may address data recovery, alternate data-processing capabilities, emergency staffing, and customer service support. Management should establish a communication plan that designates key personnel and outlines a program for employee notification. The plan should include a public relations and outreach strategy to respond promptly to customer and media reaction to system failure or unauthorized intrusions. Management should also plan for how it may respond to events outside the bank that may substantially affect customer confidence, such as an operational failure experienced by a competitor that relies on similar technology.

Additional reference should also be made to BSP Memorandum dated 22 January 2004 and 3 April 2003 on Back-up Operations Centers and Data Recovery Sites and Updated Business Continuity Plan, respectively.

f. Proper Oversight of Outsourcing Activities

Bank management should ensure that all necessary controls are in place to manage risks associated with outsourcing and external alliances. Management should ensure that vendors have the necessary expertise, experience, and financial strength to fulfill their obligations. They also should ensure that the expectations and obligations of each party are clearly defined, understood and otherwise enforceable. Management should make certain that the bank has audit rights for vendors so that the bank can monitor performance under the vendor contract.

The key elements of proper project implementation apply whether a bank relies on employees, vendors, or both to develop and implement projects. Failure to establish necessary controls may result in compromised security, substandard service, and the installation of incompatible equipment, system failure, uncontrolled costs, and the disclosure of private customer information. If a bank joins or forms

alliances with other banks or companies, management should perform adequate due diligence to ensure that the joint-venture partners are competent and have the financial strength to fulfill their obligations. Adequate bank resources will be required to monitor and measure performance under the terms of any third-party agreement. Additional reference should be made to BSP Circular No. 268 dated 05 December 2000 on Outsourcing.

Measurement and Monitoring

As part of both planning and monitoring, banks must establish clearly defined measurement objectives and conduct periodic reviews to ensure that goals and standards established by bank management are met. Goals and standards should include an emphasis on data integrity, which is essential to any effective use of technology. Information should be complete and accurate both before and after it is processed. This is a particular concern in any significant merger with other institutions or acquisition of other businesses. Control of technology projects is complex because of the difficulty in measuring progress and determining actual costs. It is important that bank management establish benchmarks that are appropriate for particular applications. Ultimately, the success of technology depends on whether it delivers the intended results.

Management should monitor and measure the performance of technology-related products, services, delivery channels, and processes in order to avoid potential operational failures and to mitigate the damage that may arise if such failures occur. Bank management should establish controls that identify and manage risks so that the bank can adequately manage them. To ensure accountability, management should specify which managers are responsible for the business goals, objectives, and results of specific technology projects or systems and should establish controls, which are independent of the business unit, to ensure that risks are properly managed. Technology processes should be reviewed periodically for quality and compliance with control requirements.

Auditing

Auditors provide an important control mechanism for detecting deficiencies and managing risks in the implementation of technology. They should be qualified to assess the specific risks that arise from specific uses of technology. Bank management should provide auditors with adequate information regarding standards, policies, procedures, applications, and systems. Auditors should consult with bank management during the planning process to ensure that technology-related systems are audited thoroughly and in a cost-effective manner.

Quality Assurance

Bank management should establish procedures to ensure that quality assurance efforts take place and that the results are incorporated into future planning in order to manage and limit excessive risk taking. These procedures may include, for example, internal performance measures, focus groups and customer surveys. Bank should conduct quality assurance reviews whenever it engages in a significant combination with another institution or acquires another business.