OCC 98-3
Subject: Technology Risk Management
Description: Guidance for Bankers and Examiners

To: Chief Executive Officers and Chief Information Officers of all National Banks, General Managers of Federal Branches and Agencies, Deputy Comptrollers, Department and Division Heads, and Examining Personnel

Purpose

The purpose of this bulletin is to provide guidance on how national banks should identify, measure, monitor, and control risks associated with the use of technology. This bulletin sets forth the OCC's expectations with respect to the management of technology-related risks and is intended to provide more consistency in how the OCC supervision by risk framework is applied to these risks. The OCC will review technology-related risks together with all other risks to ensure that a bank's risk management is integrated and comprehensive. The guidance applies both to safety and soundness and bank information system concerns. All national banks should follow the guidance in their risk management efforts.

Summary of Key Points

This bulletin contains two main parts. The first outlines the primary risks related to bank use of technology and the second describes a risk management process for how a bank 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 transaction, strategic, reputation, and compliance risk.

- The OCC expects banks to have an integrated approach to risk management to identify, measure, monitor, and control risks in an institution. Technology- related risks will be reviewed together with other bank risks within the context of the OCC supervision by risk framework to determine a bank's overall risk profile.

- When contemplating and implementing uses of technology, bank management should engage in a rigorous analytic process to identify and quantify risks, to the extent possible, and to establish risk controls to manage risk exposures.

- The technology-related risk management process involves three essential elements. A bank should (1) plan or its use of technology, (2) decide how it will implement the technology, and (3) measure and monitor risk-taking. These elements are critical to any effective technology-related risk management process of a well-managed institution, regardless of size.

Scope and Reference

The scope of this bulletin covers all significant uses of technology. It is intended to capture the full range of technology-related risks and therefore will not be applied only to new applications. For purposes of this bulletin, "technology" refers to the tools and systems that are used to store, receive, transmit, process, and recover information. This includes, but is not limited to, computer hardware and software, and telecommunications links. This bulletin and the underlying supervision by risk framework apply to all national banks regardless of size. The bulletin complements other risk management guidance issued by the OCC, including OCC 96-48, "Stored Value Card Systems," BC-177, "Corporate Contingency Planning," and BC-229, "Information Security." [Note: These OCC issuances, except for the "Stored Value Card Systems," are included in the 1996 FFIEC Information Systems Examination Handbook.] In the future, the OCC will issue additional bulletins on specific products, services, delivery channels, and other significant applications of technology, which will identify the specific risks associated with those technologies and suggest controls for managing the risks.

Contents Page

Background

For decades, banks used technology almost exclusively for back-office processing. Today, technology has moved "out front" into virtually all aspects of banking. Technology is a key aspect of many bank business decisions and many new bank products are reliant on new technologies. Uses of technology are integral to bank operations and have been a primary force in creating new competitive opportunities for banks. New and improved technology- related products and services, delivery channels, and processing options have changed the way banks make decisions, interact with customers, and process bank transactions. Although some banks have developed new products and services in-house, many have relied on vendors to develop and operate their technology-related products and services.

While new technologies have provided important benefits to banks and their customers, they also have exposed banks to new and different risks. As banks increase their dependency on technology to deliver services and process information, the risk of adverse consequences from operational failures increases. For example, some banks have taken days to recover from operational failures arising out of technology system failures. Also, as banks continue to increase their retail on-line payments, system security may pose even greater challenges to banks in the future. These and other technology-related problems could result in financial and reputation losses, which in turn could potentially threaten the safety and soundness of an institution.

Technology-Related Risks

Although banks using technology-related products, services, delivery channels, and processes can be exposed to all of the nine categories of risk outlined in the OCC supervision by risk framework, they typically are exposed to transaction, strategic, reputation, and compliance risk. [Note: As outlined in the OCC "Bank Supervision Process" booklet in the Comptroller's Handbook series the OCC's supervision by risk program is designed to focus examiner attention on the most significant risks within a particular institution and within the industry as a whole. The OCC's nine categories of risk for bank supervision purposes are: credit, compliance, foreign exchange, interest rate, liquidity, price, reputation, transaction, and strategic risk. These categories are not mutually exclusive, and any product or service may expose a bank to multiple risks. The nine risk categories provide a method of identifying, evaluating, documenting, and communicating judgments to banks about both the quantity of risk and the quality of risk management in each bank. The assessment reflects both a current and prospective view of the institution's risk profile by identifying risks in the bank using common definitions, measuring the quantity of risk using common evaluation factors, and evaluating the quality of risk management to determine if risks are adequately managed and controlled.] The other supervision by risk categories -- credit, interest rate, liquidity, foreign exchange, and price risk -- may arise under some circumstances. With banks' increased reliance on technology to manage risks, it is

important both for banks and examiners to understand how specific technologies operate and how their use or failure may expose banks to risk. The OCC expects banks to have the knowledge and skills necessary to understand and effectively manage their technology-related risks. The OCC will evaluate technology-related risks in terms of the nine categories of risks described in the OCC supervision by risk program.

Transaction Risk

Transaction risk 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. Transaction risk exists in all products and services.

Technology can give rise to transaction risk in many ways. Transaction 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 exposes a bank to transaction risk. Transaction 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, transaction 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 transaction risk.

Strategic Risk

Strategic risk 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 a 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

Reputation risk 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 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 agency transactions.

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

Compliance risk 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 parties 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, such as the Bank Secrecy Act. The use of technology to automate lending decisions also could expose a bank to compliance risk 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 programs rely are flawed or if the program design itself is flawed. In some cases, such flawed credit scoring models could result in lending patterns that violate fair lending laws and regulations.

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. Legislatures and agencies are frequently modifying their laws and regulations to accommodate new technologies. 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.

OCC Risk-Based Supervision of Bank Technology

The OCC expects bank management to identify, measure, monitor, and control its technology-related risks and, as with all other risks, to avoid excessive risk-taking that may threaten the safety and soundness of an institution. Because technology-related risks are important factors in assessing an institution's overall risk profile, the OCC's primary supervisory concern in reviewing a bank's use of technology is whether the bank is assuming a level of risk that exceeds its ability to manage and control the risk. While the risk management process outlined below is applicable to all technology-related products, services, delivery channels and processes, all such investments will not raise supervisory concerns.

The OCC will focus on business activities and decisions that may have a material impact on a bank's risk profile. Management should engage in a rigorous analytic process to identify, quantify, to the extent possible, and establish risk controls to manage risk exposure. To the extent a bank cannot quantify specific risks, management should establish a disciplined approach to assess the magnitude of potential problems and then take steps to address them.

The OCC understands and appreciates that banks currently address their technology-related needs in different ways. For example, some institutions incorporate technology planning into their overall strategic plans while others deal with technology applications on a project-by-project basis. The sophistication of the risk management process should be appropriate for the bank's level of risk exposure. This includes the materiality of the risks, the degree of risk posed by technology as compared to, and when aggregated with, other bank risks, and the overall ability of the institution to manage and control its risks. Regardless of the specific bank approach, sound risk management systems have several common fundamentals as outlined in the OCC

supervision by risk framework: risk identification, risk measurement, risk control, and risk monitoring.

Technology-Related Risk Management Process

The technology-related risk management process is designed to help a bank to identify, measure, monitor, and control its risk exposure. The process involves three essential elements. A bank should (1) plan for its use of technology, (2) decide how it will implement the technology, and (3) measure and monitor risk-taking. In reviewing a bank's risk management process, the OCC will look to see 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 will be more complex for larger institutions, particularly for those with major technology-related initiatives.

Plan

When considering whether to adopt a new technology or to upgrade existing systems, a bank should assess how it will use the technology within the context of its overall strategic goals and its market. Planning should consider issues such as the:

- Costs of development and costs related to designing, Testing, and operating the systems, both internally and through outside vendors;
- Ability to resume operations swiftly and with data intact in the event of system failure or unauthorized intrusions;
- Adequacy of internal controls, including controls for outside vendors; and
- Ability to determine when a specific risk exposure exceeds the ability of an institution to manage and control that risk.

Given the specialized expertise 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. In planning 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.

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 plans. [Note: Technology planning often involves strategic, business, and project planning. The 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.

The 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. The 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.

There are three basic components of an effective planning process for technology-related applications. The bank should (1) involve the board of directors and senior management in decision-making throughout the planning process; (2) gather and analyze relevant information regarding new and existing technologies; and (3) assess needs and review relevant options. These components serve to stimulate thoughtful analysis and to ensure coordination and project integration among all interested parties. For banks with more complex operations, the interested parties may include technology specialists, marketing representatives, business managers, and senior management.

Involve Senior Management and Board of Directors in Decision-making. The OCC will evaluate whether senior management has sufficient knowledge and skills to manage the bank's use of technology and whether senior management and the Board of Directors are sufficiently engaged in the planning process to manage the bank's technology- related risks.

Senior management's knowledge of, and involvement in, the technology planning process plays an important role in managing a bank's risks. The board of directors and senior management 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 the knowledge and skills to evaluate critically the design, operation and oversight of technology projects. The board should be fully informed by senior management, 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.

Gather and Analyze Information. The OCC will assess whether banks understand existing systems, consumer expectations, and competitive

forces in their planning for new or enhanced uses of technology. As part of this process to gather and analyze information, banks should:

- Inventory existing systems and operations. Banks should review their existing systems to determine whether they satisfy current and projected bank needs. They also should 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.

Assess Needs and Review Options. The OCC will evaluate whether bank management has carefully assessed its technology needs and reviewed its options within the context of overall planning. Management should consider carefully whether the necessary resources, time, and project management expertise is available to complete successfully 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 also should 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 use caution 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 up projects into manageable segments and establishing specific decision points as to whether a project should be modified or terminated. Planning also should 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 also should include an assessment of the cost to start, run, and terminate a project.

Implement

The OCC will evaluate whether banks have project management controls in place to ensure proper 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. Proper project implementation includes controls, policies and procedures, training, testing, contingency planning, and proper oversight of any outsourcing. Management should provide clearly defined expectations, including user and resource requirements, cost estimates, project benchmarks, and expected delivery dates. Proper project monitoring by all relevant parties is important. Project managers should inform senior management of obstacles as early as possible to ensure that proper controls are in place and corrective action can be taken to manage risk exposure.

Controls. The OCC will assess whether banks have adopted 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.

Policies and Procedures. The OCC will assess whether management has adopted and enforces appropriate policies and procedures to manage risk related to a bank's use of technology. The effectiveness of these policies and procedures depends largely 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.

Expertise and Training. The OCC will assess whether bank management has a plan to 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 adequate back -up exists if a critical person leaves. 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 outreach to customers to ensure that a bank's customers understand how to use or access a bank's technology products and services and that they are able to do so in an appropriate and sound manner.

Testing. The OCC will assess whether bank management has thoroughly tested 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 older technology 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.

Contingency Planning and Business Continuity. The OCC will review bank systems to assess whether the systems are designed to reduce bank vulnerability to system failures, unauthorized intrusions, and other problems. The OCC also will review whether back-up systems exist and have been fully maintained and tested on a regular basis to minimize the risk of system failures and unauthorized intrusions. The risk of equipment failure and human error is possible in all systems. This risk may result from sources both within and beyond the bank's control. System failures and unauthorized intrusions may result from design defects, insufficient system capacity, destruction of a facility by natural disasters or fires, security breaches, inadequate staff training, or uncontrolled reliance on vendors.

Business continuity plans should be in place before a 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 communications 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 also should 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.

Outsourcing. The OCC will assess bank management's efforts to 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. For example, 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 a combination to develop and implement projects. Failure to establish necessary controls may result in compromised security, substandard service, 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.

Measure and Monitor Performance

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. The OCC will evaluate whether bank management has established 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. The OCC will assess the adequacy of audits in identifying and managing technology-related risks. 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. The OCC will review whether bank management has established 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. The OCC also will assess whether a bank conducts quality assurance reviews whenever it engages in a significant combination with another institution or acquires another business.

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.

Responsible Office

Questions regarding this banking circular or the information it contains should be directed to the Bank Technology Unit, (202) 874-2340 or via E-mail: BT@occ.treas.gov.

James D. Kamihachi
Senior Deputy Comptroller for
Economics and Policy Analysis