RESCINDED AL 2000–2

OCC ADVISORY LETTER

Any attachments to this document are rescinded only as they relate to national banks and federal savings associations.

Subject: Technology Risk Management Lessons from Year 2000 Project

TO: Chief Executive Officers of National Banks, Federal Branches, Service Providers, and Software Vendors; Department and Division Heads, and Examining Personnel

The Federal Financial Institutions Examination Council (FFIEC) has released the attached guidance, "Lessons Learned from the Year 2000 Project." Many of the lessons learned from the Year 2000 project can be applied to improve future technology risk management processes.

Because technology-related risks are important in a financial institution's overall risk profile, the OCC expects management to identify, measure, monitor, and control its technology-related risks. Accordingly, we encourage you to consider the lessons learned outlined in the attached FFIEC document as a way to improve technology risk management.

The guidance is also available on the OCC's Web site at **www.occ.treas.gov**. For more information, contact Bank Technology at (202) 874-5920.

Mark L. O'Dell
Deputy Comptroller, Core Policy

Attachment

Federal Financial Institutions Examination Council

2000 K Street, NW, Suite 310 . Washington, DC 20006 . (202) 872-7500 . FAX (202) 872-7501

PRESS RELEASE
For Immediate Release

March 21, 2000

FFIEC Urges Financial Institutions Not to Forget Lessons Learned from Year 2000 Project

WASHINGTON, D.C. -- Bank, thrift, and credit union regulators issued today a document discussing lessons learned from the preparation for the Year 2000 date change, and urged financial institutions to incorporate the knowledge gained from that experience into future project and technology risk management.

Through the Federal Financial Institutions Examination Council (FFIEC), the federal regulators of these institutions today issued "Lessons Learned from the Year 2000 Project." In releasing the document, the FFIEC urged financial institutions to conduct their own review of lessons from the Y2K effort and incorporate them in future project management processes and technology risk management. The FFIEC believes that the best-prepared institutions possessed most or all of 10 characteristics:

- Senior management and director involvement to ensure that the project plans were clearly defined, supported and monitored;

- Consolidation, elimination or integration of technology on an enterprise-wide basis by developing current inventories of information technology systems and applications;

- Improved oversight of service providers, software vendors and consultants;

- More formalized and effective strategies and standards for testing information technology systems;

- Detailed contingency plans that analyzed the effect of potential system failures on core business processes (e.g., deposit taking, lending, fiduciary services, etc.);

- Better safeguards to detect fraudulent, malicious, and negligent acts from both internal and external sources;

- Review of testing and contingency planning processes by internal auditors;

- Open information sharing for developing strategies and to respond to media reports or perceptions that could reduce public confidence in the financial services industry;

- Improved public relations with customers; and

- Thorough legal review to assist in vendor management, documentation retention, and legal defense.

The FFIEC is sending the lessons document to directors and chief executive officers of all federally supervised financial institutions, service providers, software vendors, federal branches and agencies, senior management of each FFIEC agency, and all examining personnel.

###

Federal Financial Institutions Examination Council

2000 K Street, NW, Suite 310. Washington, DC 20006. (202) 872-7500. FAX (202) 872-7501

Lessons Learned from the Year 2000 Project

March 21, 2000

To: The Board of Directors and Chief Executive Officers of all federally supervised financial institutions, service providers, software vendors, federal branches and agencies, senior management of each FFIEC agency, and all examining personnel.

Purpose

The Year 2000 project provided many valuable lessons that can be applied to future project management processes and technology risk management. The purpose of this guidance is to share those lessons with the industry. To ensure that the lessons learned from the Year 2000 project have lasting value, the FFIEC encourages management to conduct its own review of lessons from the Year 2000 effort and incorporate these lessons, where appropriate, in future technology risk management practices.

Background

The Year 2000 project was one of the most expensive and resource-intensive information technology challenges ever faced by the financial services industry. The project posed a technology-based problem that had to be managed on an enterprise-wide basis by more than technology experts. It transcended corporate boundaries and hierarchies and required organizations to work together to review information technology (IT) systems and business practices and develop a comprehensive strategy to address technology-related risks and business continuity plans.

Lessons Learned

The FFIEC has determined that the best-prepared institutions possessed most or all of the following characteristics:

Senior Management/Director Involvement and Interdisciplinary Teams

The commitment and involvement of senior management and board of directors from the early stages of the Year 2000 project to its completion was critical to ensuring that all aspects of the project were carefully considered and that the project was clearly defined, supported, funded and monitored. Many institutions established new reporting mechanisms to keep senior management apprised of progress and to manage risks. These reporting mechanisms helped to keep Year 2000

projects on schedule and to ensure that adequate resources were available. Quality assurance reviews, benchmarking, and internal audits also were established to ensure risks were properly managed. As part of both planning and monitoring, financial institutions established clearly defined measurement objectives and conducted periodic reviews to ensure that these goals and standards were met. The efforts of interdisciplinary teams, comprised of experts from IT systems, affected business units, law departments, and corporate communications helped institutions to better manage risks. These teams helped to facilitate critical phases of the project and emphasize the priority of the project through the entire organization.

Comprehensive IT Inventories

Financial institutions developed current inventories of information technology systems and applications. This enabled many institutions to consolidate, eliminate, or integrate technology projects on an enterprise-wide basis. Effective planning served as a catalyst for modernizing computer systems and integrating new systems with relevant legacy systems. Comprehensive inventories also fostered better risk evaluation and decision-making, ensuring that IT systems were consistent with current operating strategies.

Improved Vendor Management

Financial institutions established better due diligence processes to oversee service providers and software vendors that provide mission-critical services and products. Many financial institutions that relied upon service providers, software vendors, and consultants found that they had substantial risk exposures related to vendor management that were not adequately measured, monitored, managed, or controlled. Many financial institutions expanded their analysis of the ability of service providers, software vendors, and consultants to fulfill their contractual obligations. In addition, institutions took steps to improve communications and clarify roles, responsibilities, and contractual obligations.

Effective Testing Strategies

Formalized testing strategies improved the overall testing process during the Year 2000 project by recognizing interdependencies between IT systems and other business units. Many institutions developed formal strategies and standards for testing information technology systems for the first time. Financial institutions, service providers and software vendors also improved testing processes and environments by creating more efficient testing methodologies and change management practices.

Detailed Contingency Planning

Many financial institutions reported significant benefits from the development of Year 2000 contingency and "event management" plans. Contingency planning evolved from a largely theoretical exercise to a problem solving and training tool to help organizations respond promptly to operational failures and natural disasters. Institutions developed more detailed contingency plans by analyzing the effect of potential system failures on core business processes (e.g., deposit taking, lending, fiduciary services, etc.); determining the minimum level of output and services for each core business process; testing the contingency plans; and validating the results through independent parties. They also recognized the need to review and plan for contingencies related to all aspects of

an institution's operating environment, including IT systems (e.g., mainframe systems, desktops, networks) and non-IT systems (e.g., facilities, buildings). Simulations, "table top" exercises, and other forms of tests reduced the time needed to respond to operational problems and improved decision-making and communications among senior management, corporate communications officials, and business units.

Strong Internal Controls and Security

Financial institutions focused attention on protecting critical IT systems during the Year 2000 project by establishing better safeguards to detect fraudulent, malicious, and negligent acts from both internal and external sources. Control points included satisfactory internal audits that covered facilities, personnel, policies and procedures, telecommunications, system software, application software, service providers and software vendors. Important precautions to protect system security included instituting enhanced security access restrictions, background checks on employees and contractors, enforcing appropriate separation of duties, and generating effective audit trails. Financial institutions also developed contact lists to get advice on how best to respond to intrusions/attacks and to alert others about intrusions/attacks on computer and telecommunication systems.

Financial institution internal auditors provided an important control mechanism for detecting deficiencies and managing risks in the implementation of the Year 2000 project. Many institutions before the Year 2000 project did not treat information technology audits as critical, or did not focus adequate attention on assessing the audits. Internal auditors commented early in the testing and contingency planning processes and independently validated tests and contingency plans. They also reviewed the documentation of results of tests and followed-up on outstanding items and re-tests.

Open Information Sharing

The Year 2000 project was a unique demonstration of cooperative and open communication among individuals and organizations across competitive lines and regulatory boundaries. Financial institutions worked together in unprecedented fashion with other financial institutions, service providers, software vendors, trade associations, regulators, and other industries to share information and strategies and to respond to media reports or perceptions that could decrease public confidence in the financial services industry.

Improved Public Relations

The Year 2000 project afforded financial institutions many opportunities to communicate with customers, building on previously established relationships and establishing new ones. The financial industry took great steps to ensure that the public had accurate information about the Year 2000 readiness of the industry. For example, institutions sent Year 2000 information in monthly and quarterly statements; displayed Year 2000 posters in lobbies; posted information signs at ATMs; advertised in local newspapers, radio and television; and created special Year 2000 web sites.

Thorough Legal Review

Many institutions benefited from involving legal counsel on their project management team. Legal counsel reviewed contracts as part of vendor management and advised management on the

availability of various safe harbors under the "Year 2000 Information and Readiness Disclosure Act." By involving legal counsel in contract review early in the process, some institutions avoided contractual issues with service providers and software vendors. Many institutions also established consistent approaches to documentation retention and record keeping as part of the institution's legal defense strategy for demonstrating due diligence in preparing for the Year 2000. In-house counsel also benefited from working closely with the Chief Technology Officer and Chief Information Officer on a project that cut across a range of different disciplines.