AL 97-10
Subject: Year 2000 Business Risk

RESCINDED

TO: Chief Executiv Offices of National Banks, Federal Branches and Data-Processing Centers, Department and Division Heads, and Examining Personnel

This advisory is to alert you to the recent release of FFIEC "Safety and Soundness Guidelines Concerning Year 2000 Business Risk" (attached). These guidelines supplement the FFIEC Interagency Statement and examination procedures, "Year 2000 Project Management Awareness," issued in May 1997. The safety and soundness guidelines provide additional information about the expectations of regulators for bank senior management and boards of directors in overseeing and managing their year 2000 projects.

Any attachments to this document are rescinded only as they relate to national banks and federal savings associations.

Year 2000 problems present corporate-wide challenges for financial institutions. The FFIEC safety and soundness guidance underscores the responsibility of bank senior managers and boards of directors to actively manage efforts to correct year 2000 problems. They must devote sufficient resources to ensure that the remediation efforts are given top priority, and that the project receives the quality personnel and timely support it requires. Senior bank managers must provide board members with status reports, at least quarterly, on the year 2000 compliance efforts of both in-house teams and outside vendors.

Banks also need to properly manage their vendor relationships. The FFIEC guidance clarifies vendor management issues discussed in the May FFIEC Interagency Statement and explains that formal certification to financial institutions from vendors that their products and services are year 2000 compliant may not be sufficient to prevent potential problems. Accordingly, the FFIEC guidance says banks do not need to obtain formal certification of year 2000 compliance from their vendors. Rather, banks need to have good communication channels with their vendors, and conduct their own due diligence inquiries concerning their vendors' year 2000 readiness. Banks also should implement their own internal testing or verification processes for vendor products and services to ensure that the banks' different computer systems function properly together.

In addition, management should ensure that year 2000 contingency plans are developed for all mission-critical applications and systems. Time frames for year 2000 contingency plans should be consistent with those outlined in the FFIEC Interagency Statement. By December 31, 1998, all programming changes should be completed and testing should be well underway for mission-critical systems. Also, when OCC examiners conduct quarterly reviews of year 2000 compliance activities, they will review each bank's contingency plans to ensure that they include alternative solutions and reasonable trigger dates for implementing those solutions, if necessary.

For further information on year 2000 issues, contact the Bank Technology unit at
(202) 874-2340.

James D. Kamihachi
Senior Deputy Comptroller
Economics and Policy Analysis
Date: December 19, 1997

Attachment

Federal Financial Institutions Examination Council

Press Release

For Immediate Release December 17, 1997

FFIEC ISSUES GUIDANCE ON YEAR 2000 BUSINESS ENTERPRISE RISK

WASHINGTON, D.C. -- The Federal Financial Institutions Examination Council (FFIEC) today issued safety and soundness guidance on business-wide risk posed to financial institutions by the Year 2000 problem. The guidance underscores that Year 2000 preparation is not only an information systems issue, but an enterprise-wide challenge that must be addressed at the highest level of a financial institution. The guidance lays out what the financial institution regulators expect from senior management and boards of directors in overseeing and managing their Year 2000 projects.

"Financial institutions that treat the Year 2000 only as a technology issue will be caught short," said Eugene Ludwig, chairman of the FFIEC. "We want to emphasize to senior management and the boards of directors of financial institutions that we expect this issue to be addressed across the full spectrum of financial institution operations."

The purpose of these safety and soundness guidelines is to underscore the responsibilities of senior management and the boards of directors for addressing the business risks associated with the Year 2000. This includes managing the internal and external risks presented by providers of data-processing products and services (vendors), business partners, counterparties, and major loan customers.

The guidance instructs senior management to provide the board of directors with status reports, at least quarterly, on the efforts being made to reach Year 2000 goals both internally and by the institution's major vendors. Senior managers and directors must allocate sufficient resources to ensure that high priority is given to seeing that remediation plans are fulfilled, and that the project receives the quality personnel and timely support it requires.

The guidance also makes clear that regulators are not asking financial institutions to obtain certification from their vendors of Year 2000 compliance. Rather, an institution needs to implement its own internal testing or verification processes for vendor products and services to ensure that its different computer systems function properly together.

The guidance underscores the importance of contingency planning in Year 2000 preparations. If a financial institution's Year 2000 corrections will not be completed on schedule, management should be ready to implement contingency plans to ensure that all mission-critical renovations or replacements are made within the timeframe established in the FFIEC *Year 2000 Project Management Awareness* guidelines, issued in May.

The FFIEC member agencies strongly encourage financial institutions and their trade organizations to work collectively to address issues pertaining to the year 2000. Effective industry cooperation can help reduce costs and improve results. By working together, financial institutions can share ideas, influence vendors, develop best management practices, and maintain their competitiveness with other industries.

The FFIEC prescribes uniform principles, standards and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

[Top of Page] [Press Releases] [FFIEC Home Page]

FFIEC
Federal Financial Institutions Examination Council

Safety And Soundness Guidelines Concerning The Year 2000 Business Risk

December 17, 1997

To:

The Board of Directors and Chief Executive Officers of all federally supervised financial institutions,providers of data services, senior management of each FFIEC agency, and all examining personnel

Background:

On May 5, 1997, the FFIEC issued an interagency statement entitled "Year 2000 Project Management Awareness" (Interagency Statement) focusing on the project management process and other significant Year 2000 issues. Although the Interagency Statement provided a detailed overview of the Year 2000 project management process, subsequent discussions with financial institutions, vendors and consultants indicate the need for additional guidance regarding regulatory expectations of senior management and the board of directors concerning the business-wide implications of these issues.

Purpose:

The purpose of these safety and soundness guidelines is to outline the responsibilities of senior management and the board of directors for addressing the business risks associated with the Year 2000 problem. Senior management and the board of directors should actively manage efforts to plan, allocate resources and monitor progress to correct Year 2000 problems. This includes managing the internal and external risks presented by providers of data processing products and services (vendors), business partners, counter parties, and major loan customers.

Return to top

Summary:

These guidelines outline the agencies' expectations in the following areas:

- The Year 2000 problem is much more than a technology issue; it is an enterprise-wide challenge. Senior management and the board of directors must be actively involved in overseeing internal Year 2000 efforts and monitoring the business risks posed by vendors, business partners, counter parties, and major loan customers.

- In order to be fully informed and provide effective direction, management must provide the board with status reports, at least quarterly, on the financial institution's Year 2000 efforts. Reporting must include information on the institution's internal Year 2000 corrective efforts and the ability of the institution's major vendors to provide Year 2000 ready products and services.

- The regulatory agencies are clarifying the Interagency Statement's guidance that suggested financial institutions seek certification from their vendors that their products and services are Year 2000 compliant. Formal certification is not required as it alone is not sufficient to ensure that a product or service would operate properly in the unique environment of many user institutions. Instead, financial institutions should (a) communicate with their vendors and conduct due diligence inquiries

concerning Year 2000 readiness and also (b) implement their own appropriate internal testing or verification processes pertaining to these vendor products and services to ensure that their systems and data function properly together. Financial institutions should develop contingency plans for all vendors that service mission critical applications and establish a trigger date for implementing alternative solutions should the vendor not complete its conversion efforts on time.

- The Year 2000 problem requires an extensive project planning process to ensure that management addresses all business critical issues in a timely and prudent manner. Management must allocate sufficient human and financial resources to the project and should develop/monitor contingency plans for use if Year 2000 corrective efforts do not materialize as expected.

- To increase the probability of successfully resolving Year 2000 problems, financial institutions should work together to find common solutions by sharing successful practices, common testing methodologies and other non-proprietary information.

Return to top

Enterprise Challenge:

The Year 2000 problem presents corporate-wide challenges for financial institutions, their vendors, business partners, counter parties, and customers. However, the regulatory agencies are concerned that many financial institutions view the Year 2000 issue solely as an information system (IS) problem rather than a broader, enterprise-wide challenge. Many institutions may not have adequately funded their Year 2000 programs and may lack the necessary resources to properly address the issue.

The board of directors should ensure that senior management is taking an enterprise-wide approach to address Year 2000 problems and must provide sufficient resources to resolve Year 2000 problems. For example:

- As the Year 2000 will affect most, if not all, of an institution’s accounting and risk control systems, there should be close coordination between business units and the institution’s operational and risk management functions as conversion programs are executed.

- Financial institutions relying on vendors for information processing services or products should determine their vendors’ progress in resolving Year 2000 issues and the readiness of their own systems and data for appropriate testing. Parties throughout the institution should be involved to coordinate readiness efforts and to develop contingency plans.

- The interdependencies of a financial institution's information systems will require comprehensive testing of applications with all internal and external systems that share information. Senior management should monitor the testing of all mission critical systems.

- The approach of the Year 2000 creates potentially adverse effects on the creditworthiness of borrowers. Corporate customers who have not considered Year 2000 issues may experience a disruption in business, resulting in potential financial difficulties affecting their creditworthiness. Financial institutions should develop processes to identify, assess, and control the potential Year 2000 credit risk in their lending and investment portfolios. The regulatory agencies are preparing additional guidance with respect to their expectations of senior management concerning these indirect risks and other important topics.

Return to top

Reporting to the Board:

The board of directors must oversee the institution's Year 2000 efforts. Senior management must manage the project on a day-to-day basis, ensuring the appropriate prioritization of resources and establishment of proper benchmarks and time lines. The board must, at a minimum, require quarterly status reports from management that detail the organization's progress in addressing Year 2000 issues. The board should be immediately notified if the project fails to meet critical benchmarks.

The nature and extent of reporting should reflect the complexity of the institution's operations. Reports should include, but not necessarily be limited to, updates concerning the:

- Overall progress of the Year 2000 project, including any new efforts initiated since the last report.
- Progress plotted against the institution's Year 2000 project plan, including comparisons against performance benchmarks.
- Status of efforts by key vendors, business partners, counter parties, and major loan customers to address Year 2000 issues, including any weaknesses discovered and critical decision dates.
- Results of internal and external testing of information processing applications, databases, and systems.
- Contingency planning efforts that outline alternative courses of action in the event existing internal systems or external systems provided by vendors will not be ready for the Year 2000.

Reports to the board, for institutions that are responsible for the renovation of their own mission critical applications[1], should also be tailored to the complexity of its applications and should provide information that:

- Identifies the total number of applications inventoried during the assessment phase and details the number of mission critical applications in each stage of the five step project management process outlined in the Interagency Statement.
- Informs the board about the progress being made to complete the renovation, testing and implementation of mission critical applications.
- Identifies the number of mission critical applications grouped by the intended resolution strategy (e.g., repair, install vendor upgrade, eliminate/retire, outsource, test only).
- Summarizes the results of internal and external testing.

Board minutes should reflect, as appropriate, any material action taken by the board to address Year 2000 issues or concerns. Board reporting should be available for review by examiners during onsite and offsite supervisory activities.

Return to top

Clarification of Certification Requirement:

The Interagency Statement suggested that financial institutions obtain certification from their vendors when products and services are Year 2000 compliant. However, the regulatory agencies recognize that certification alone is not sufficient to provide adequate assurance that a

product will operate properly in the unique environments of the many user financial institutions. Only a comprehensive test of all internal and external systems and system interdependencies by each user financial institution will ensure that they will function properly together. Therefore, formal certification is not required. Instead, financial institutions should (a) communicate with their vendors and conduct due diligence inquiries concerning Year 2000 readiness and also (b) implement their own appropriate internal testing or verification processes pertaining to these vendor products and services to ensure that their systems and data function properly together. They should monitor closely their vendor's progress in meeting target deadlines. The vendor's plan should allow adequate time for user testing in a Year 2000 environment. Topics that should be addressed with vendors include:

- Dates that products will be Year 2000 ready and available for testing.
- Products that will not be Year 2000 ready, or will no longer be supported.
- Methods used to renovate the product or the system to address Year 2000 (e.g., field expansion, windowing).
- The pivot year, if the windowing method is used. [2]
- Any efforts that require coordination between the institution, its vendor and any other parties involved in external testing.
- Vendor guidance on user testing of products.

Financial institutions should develop contingency plans for all vendors that service mission critical applications and establish a trigger date for implementing alternative solutions should the vendor not complete its conversion efforts on time. These plans should consider the institution's own level of preparedness as well as that of their service providers. Contingency plans should be reviewed at least quarterly and adjusted, if necessary, to reflect current circumstances.

In establishing relevant trigger dates, management should have a thorough understanding of the complex interrelationships between its systems and those of its vendors. An institution also should consider the time necessary to convert the existing system to one that is ready for the Year 2000, the staff training time needed to implement an alternative system, and the availability of alternative systems. If, after a thorough analysis, it appears that the institution's Year 2000 conversions, or those of its vendors, will not be completed on time, management should be ready to implement its contingency plans. If success is in doubt for complex applications, it may be necessary to begin implementation of the contingency plan while continuing to work on the desired solution. Additionally, it may be necessary to begin renovation on an existing system, if timely implementation of a replacement system is not assured.

For in-house developed applications, the contingency plan should identify how the institution will transition to an alternate system or to an external vendor. For institutions that rely on vendors, the contingency plan should identify alternative suppliers and outline migration plans. In addition, time frames for Year 2000 contingency plans should be consistent with the time frames set forth in the Interagency Statement. The statement establishes December 31, 1998, as the date that institutions will have completed programming changes and have testing well underway for mission-critical systems.

Return to top

Project Planning and Management:

The Year 2000 problem requires extensive project planning to ensure proper allocations of resources, and to ensure management accountability. The project plan should be formally adopted, enterprise-wide in scope, and contain clearly defined objectives and deadlines. The project plan, at a minimum, should include the following:

- The tasks to be accomplished throughout the term of the project.
- Resource requirements and individuals assigned responsibility for various phases of the project.
- Specific dates for completion of key elements of the project.
- Strategy for responding to inquiries from customers and business partners regarding the institution's Year 2000 readiness.

Senior management should actively manage resources to ensure that the project remains on schedule. Management should implement processes that monitor the Year 2000 efforts of its vendors, business partners, counter parties, and major loan customers.

The regulatory agencies are concerned that many financial institutions and service providers will underestimate the costs of Year 2000 projects, especially those costs associated with the testing phase. As the Year 2000 approaches, the demand for technical resources will likely rise and the supply of these resources is expected to diminish, thereby increasing costs. Financial institutions must exercise appropriate due diligence in their budget planning to ensure that they have sufficient financial and human resources to complete their Year 2000 plans in a timely manner.

Given the nature and extent of the Year 2000 challenge, management may need to adjust resources throughout the life of the project. If adjustments are needed, management must redefine the project's scope, and, if appropriate, change the priorities of other data processing projects.

Industry Coordination:

The FFIEC member agencies strongly encourage financial institutions and their trade organizations to work collectively to address issues pertaining to the Year 2000. Effective industry cooperation can help reduce costs. By working together, financial institutions can share ideas, influence vendors, develop best management practices, and maintain their competitiveness with other industries. Financial institutions should consider enlisting industry associations and accounting firms for guidance. If the industry is to be successful in meeting the problems posed by the Year 2000, financial institutions will have to work cooperatively to share effective practices, common testing methodologies and other non-proprietary information.

Return to top

Footnotes:

1 An application or system is mission critical if it is vital to the successful continuance of a core business activity. An application may be mission critical if it interfaces with a designated mission critical system.

2 Windowing for the Year 2000 involves the establishment of a "pivot year". Dates that are greater than or equal to the pivot year are interpreted to be 19xx. Dates that are less than the pivot year are interpreted to be 20xx.

Maintained by *FFIEC*. All suggestions regarding this site may be forwarded via e-mail.
Last Updated: December 30, 1997