RESCINDED

AL 98-03
Subject: Year 2000 Guidance on Customer Risk and Vendor Due Diligence
Date: March 17, 1998

Any attachments to this document are rescinded only as they relate to national banks and federal savings associations.

TO: Chief Executive Officers 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 two FFIEC interagency statements on the Year 2000 problem. "Guidance Concerning the Year 2000 Impact on Customers" and "Guidance Concerning Institution Due Diligence in Connection with Service Provider and Software Vendor Year 2000 Readiness" supplement previous FFIEC interagency statements by providing additional information on overseeir and managing Year 2000-related risk for bank customers and for vendors that provide mission-critical products and services.

"Guidance Concerning the Year 2000 Impact on Customers" describes the responsibilities of a financial institution's senior management and board of directors for assessing the risks arising from the failure of the institution's customers to address their Year 2000 vulnerabilities. A financial institution can face increased credit, liquidity, or counterparty trading risk when its customers encounter Year 2000-related problems. Year 2000 risk may result from the failure of a customer to properly remediate its own systems and from Year 2000 problems that are not addressed by the customer's suppliers and its clients. By June 30, 1998, senior management should have implemented a process which identifies, assesses and controls the Year 2000 risk posed by their customers.

"Guidance Concerning Institution Due Diligence in Connection with Service Provider and Software Vendor Year 2000 Readiness" addresses the process for determining the ability of a bank's service providers and software vendors to become Year 2000 ready.

The vendor due diligence process should enable management to:

identify and assess the mission-critical services and products provided by service providers and software vendors;

identify and articulate the obligations of the service provider or software vendor and the institution for achieving Year 2000 readiness;

test the remediated services and products in the institution's own environment;

adopt contingency plans for each mission-critical service and product; and

establish monitoring procedures to verify that the service provider or software vendor is taking appropriate action to achieve Year 2000 readiness.

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

Emory Wayne Rushton
Senior Deputy Comptroller
Bank Supervision Policy

Attachments

FFIEC Press Release

For Immediate Release
March 17, 1998

# FFIEC ISSUES GUIDANCE ON VENDORS AND CUSTOMERS' YEAR 2000 RISK

The Federal Financial Institutions Examination Council (FFIEC) today issued additional guidance for financial institutions on risks they face due to the Year 2000 date change -- risk from service providers and software vendors and from institutions' customers. Today's guidance follows previous FFIEC Year 2000 statements on project management and business risk. "Regulators want to make sure senior management and boards of directors are fully aware of the wide range of risks that the Year 2000 date change poses for their institutions," said FFIEC Chairman Eugene A. Ludwig. "Regulators have made a major commitment to this challenge and all financial institutions are expected to do the same."

## Vendor Due Diligence Guidance

Today's FFIEC guidance on Year 2000 risks from service providers and software vendors calls for financial institutions to develop a due diligence process that includes identifying mission-critical services and products provided by service providers and software vendors, monitoring procedures to verify that service providers and vendors are taking appropriate Year 2000 action, establishing contingency plans, and testing of these services and products within the environment of the financial institution to the extent possible.

The guidance encourages financial institutions to join other financial institutions through user groups to evaluate and test service providers and software vendors' Year 2000 efforts. These joint efforts may help financial institutions to solicit information and demand performance from service providers and software vendors that provide mission-critical products and services. Financial institutions should develop contingency plans for all mission critical systems and ensure that they pursue alternative means of achieving Year 2000 readiness in the event the service provider or software vendor cannot complete critical efforts by "trigger dates."

As part of the FFIEC's efforts, the FFIEC agencies are conducting examinations of service providers and will provide the results of these examinations to the federally insured financial institution clients of these servicers. The FFIEC agencies also will inspect software vendors that agree to examinations and, where software vendors consent, the agencies will release the results of those examinations to serviced institutions. The agencies, however, will not certify service providers or software vendors as Year 2000 compliant as a result of these reviews.

Customer Risk Guidance

Today's customer risk guidance outlines a due diligence process that will help financial institutions identify material customers, evaluate their Year 2000 preparedness, assess their Year 2000 customer risk, and implement controls to manage the risk. A financial institution can face increased credit, liquidity, or counterparty trading risk when its customers encounter Year 2000-related problems. By June 30, 1998, senior management should implement the due diligence process. By September 30, 1998, Year 2000 assessments, based on this due diligence process, should be substantially completed. The customer risk guidance includes sample forms and questionnaires to assist financial institutions in evaluating the Year 2000 preparedness of their customers.

The guidance recognizes that the due diligence process will vary among financial institutions, depending on the size of an institution and the size and technological sophistication of its customers. The FFIEC identifies three major types of customers: funds takers, funds providers, and capital market/ asset management counterparties. For funds takers, such as borrowers and bond issuers, the guidance focuses on assessing how the Year 2000 will affect their ability to meet the terms of contracts.

The guidance notes that Year 2000 problems in the second group of customers, funds providers, can increase an institution's liquidity risk. Year 2000 due diligence plans for this group should focus particular attention to funding concentrations, including concentrations from one provider or group of providers.

Steps to limit Year 2000 risk from a third source -- counterparties and capital markets -- may include requirements for additional collateral or netting arrangements on contracts. The guidance underscores that failure by a capital market customer to meet its obligations because of the Year 2000 problem could cause liquidity problems and, in some cases, total loss on financial contracts.

The FFIEC will issue shortly two additional Year 2000 policy statements on testing and contingency planning.

# # #

# GUIDANCE CONCERNING
# THE YEAR 2000 IMPACT ON CUSTOMERS

To: The Boards of Directors and Chief Executive Officers of all federally supervised financial institutions, Department and Division Heads of each FFIEC agency, and all Examining Personnel.

## BACKGROUND

The Federal Financial Institutions Examination Council (FFIEC) has issued three statements providing guidance on the Year 2000 problem. Two interagency statements were issued in June 1996 and May 1997 to address the key phases of the Year 2000 project management process. The most recent guidance, published in December 1997, outlined the specific responsibilities of senior management and the board of directors to address risks associated with the Year 2000 problem.

## PURPOSE

The purpose of this guidance is to assist financial institutions in developing prudent risk controls to manage the Year 2000-related risks posed by their customers. This guidance describes a variety of approaches for a financial institution's senior management and board of directors to assess the risks arising from the failure or inability of the institution's customers to address their Year 2000 vulnerabilities. This guidance outlines the due diligence process that financial institutions should adopt to manage their Year 2000- related risks arising from relationships with three broad categories of customers: funds takers, funds providers, and capital market/asset management counterparties.

## SUMMARY

Key points addressed in this guidance include:

A financial institution can face increased credit, liquidity, or counterparty trading risk when its customers encounter Year 2000-related problems. These problems may result from the failure of a customer to properly remediate its own systems and from Year 2000 problems that are not addressed by the customer's suppliers and clients. By June 30, 1998, senior management should have implemented a due diligence process which identifies, assesses and establishes controls for the Year 2000 risk posed by customers. By September 30, 1998, the assessment of individual customers' Year 2000 preparedness and the impact on an institution should be substantially completed.

The due diligence process outlined in this guidance focuses on assessing and evaluating the efforts of an institution's customers to remediate their Year 2000 problems. Year 2000 issues related to the institution

exchanging data with its customers should be addressed as a part of the institution's internal Year 2000 project management program.

The guidance recognizes that each institution must tailor its risk management process to its size, its culture and risk appetite, the complexity of its customers, and its overall Year 2000 risk exposure. The FFIEC understands that these differences will affect the risk management programs developed by financial institutions. However, financial institutions must evaluate, monitor, and control Year 2000-related risks posed by funds providers, funds takers, and capital market/asset management counterparties.

The institution's due diligence process should identify all customers representing material Year 2000-related risk, evaluate their Year 2000 preparedness, assess the aggregate Year 2000 customer risk to the institution, and develop appropriate risk controls to manage and mitigate Year 2000 customer risk.

Risk management procedures will differ based on a variety of factors, including the institution's size, risk appetite and culture, the complexity of customers' information and operating systems, and the level of its own Year 2000 risk exposure. The Year 2000 due diligence processes used by smaller institutions may not be as extensive or formal as those in larger institutions where customers may be more dependent upon information technology.

The attached appendices provide examples of processes used by financial institutions to manage Year 2000-related customer risk.

An institution's management should provide quarterly reports to the board of directors that identify material customers who are not effectively addressing Year 2000 problems. The reports should summarize the action taken to manage the resulting risk.

OVERVIEW

The Year 2000 problem presents many challenges for financial institutions and their customers. The FFIEC recognizes that risk management procedures will vary depending on the institution's size, its risk appetite and culture, the complexity of customers' information and operating systems, and the level of its own Year 2000 risk exposure. For example, customers of small community financial institutions may not depend on computer-based information systems to the same extent as large business customers of large financial institutions. As a result, Year 2000 due diligence processes used by these institutions may not be as extensive or formal as those in institutions whose customers may be more dependent upon information technology. Senior management should oversee the development and implementation of a due

diligence process which is tailored to reflect the Year 2000 risk in their institution's customer base.

Three major types of customers may expose a financial institution to Year 2000-related risks. They include funds takers, funds providers, and capital market/asset management counterparties.

Funds Takers

Funds takers include borrowers and bond issuers that borrow or use bank funds. Failure of fund takers to address Year 2000 problems may increase credit risk to a financial institution through the inability of fund takers to repay their obligations.

Funds Providers

Funds providers provide deposits or other sources of funds to a financial institution. Liquidity risk may result if a funds provider experiences a Year 2000-related business disruption or operational failure and is unable to provide funds or fulfill funding commitments to an institution.

Capital Market/Asset Management Counterparties

Capital market and asset management counterparties include customers who are active in domestic and global financial markets. Market trading, treasury operations, and fiduciary activities may be adversely affected if a financial institution's capital market and asset management counterparties are unable to settle transactions due to operational problems caused by the Year 2000 date change.

GENERAL RISK CONTROL GUIDELINES

By June 30, 1998, financial institutions should establish a process to manage the Year 2000 risks posed by its customers. The process should: (1) identify material customers; (2) evaluate their Year 2000 preparedness; (3) assess their Year 2000 risk to the institution; and (4) implement appropriate controls to manage and mitigate their Year 2000-related risk to the institution. The assessment of individual customers' Year 2000 risk and their impact on an institution should be substantially completed by September 30, 1998. Year 2000 issues related to data exchanges between the institution and customers should be addressed as a part of an institution's internal Year 2000 project management program.

Identify Material Customers

Management should identify customers that represent material risk exposure to the institution, including international customers. Material risk exposure may depend on:

- Size of the overall relationship;
- Risk rating of the borrower;
- Complexity of the borrower's operating and information technology systems;

- Customer's reliance on technology for successful business operations;
- Collateral exposure for borrowers;
- Funding volume or credit sensitivity of funds providers; and
- Customer's dependence on third party providers of data processing services or products.

Assess Preparedness of Material Customers

The impact of Year 2000 issues on customers will differ widely. Smaller financial institutions may find that most of their material borrowers use either manual systems or depend on commercial software products and services. The evaluation of Year 2000 preparedness for these customers will be less involved and may not require additional risk management oversight. To ensure consistent information and a basis for comparisons among customers, management should address the following.

- Train account officers to perform a basic assessment of Year 2000 risk of customers.
- Develop a standard set of questions to assess the extent of a customer's Year 2000 efforts. Appendices A - D contain samples of forms some financial institutions use to evaluate customer Year 2000 preparedness. Financial Institutions are not required to use these forms, although they provide useful examples of methods to evaluate customer preparedness.
- Update the status of a customer's Year 2000 efforts periodically, but at least semi-annually. For customers that represent significant Year 2000 exposure to the institution, quarterly updates may be necessary.
- Document Year 2000 assessment conclusions, subsequent discussions, and status updates in the institution's customer files.

Evaluate Year 2000 Risk to the Institution

After identifying all customers representing material Year 2000 risk and evaluating the adequacy of their Year 2000 programs, management should assess the Year 2000 risk posed to the institution by these customers, individually and collectively. Management should determine whether the level of risk exposure is high, medium, or low. Management also should provide quarterly updates to the board of directors on customers that are not addressing Year 2000 problems effectively and discuss the actions taken by the institution to control the risk.

Develop Appropriate Risk Controls

Once the institution has evaluated the magnitude of Year 2000 risk from its customers, management must develop and implement appropriate controls to manage and mitigate the risk. Senior management should be active in developing risk mitigating strategies and ensure that effective

procedures are implemented on a timely basis to control risk.

## SPECIFIC RISK CONTROL GUIDELINES

The specific risk controls an institution implements will vary depending on the size of the institution, its risk appetite and culture, the complexity of customers' information and operating systems, and its own level of Year 2000 risk exposure. Different risk management controls may be needed to address unique and material Year 2000 issues that arise from business dealings with different categories of customer.

### Funds Takers

An institution's Year 2000 risk management controls for funds takers should focus on limiting potential credit risk by ensuring that Year 2000 problems do not prevent a borrower or bond issuer from meeting the terms of its agreements with the institution. Controls to manage an institution's exposure to its funds takers should address underwriting, documentation, credit administration, and the allowance for loan and lease losses (ALLL). These same factors also should be considered, where appropriate, when evaluating risk posed by an institution's capital market and asset management counterparties.

- Underwriting

  During any underwriting process, management should evaluate the extent of the borrower's Year 2000 risk. Specifically, management should:

  - Ensure that underwriters are properly trained and have sufficient knowledge to perform a basic assessment of Year 2000 customer risk. There are a number of resource materials available that will assist in informing lenders of Year 2000 issues. State and national trade associations have prepared materials to assist lenders in understanding customer risk created by the Year 2000. Additional information is available on the Internet and can be located by searching on the words "Year 2000".

  - Evaluate whether Year 2000 issues will materially affect the customer's cash flows, balance sheet, or supporting collateral values. As a part of the assessment and based on materiality, management should consider the complexity of the customer's operations; their dependence on service providers or software vendors; the extent of management oversight of the Year 2000 project; the resources the customer has committed to the project; and the date the customer expects to complete Year 2000 efforts.

  - Control credit maturities or obtain additional collateral, as appropriate, if credit funding is

to be continued for high-risk customers.

- Documentation
  Proper loan documentation provides an effective means to monitor and manage the Year 2000 risk posed by borrowers. Loan documents should reflect the degree of risk posed by customers. Institutions should consider incorporating some or all of the following into loan agreements:

  - Representations by borrowers that Year 2000 programs are in place;
  - Representations that borrowers will disclose Year 2000 plans to the lender, provide periodic updates on the borrower's progress of the Year 2000 program, and provide any assessment of the borrower's Year 2000 efforts conducted by a third party;
  - Audits that address Year 2000 issues;
  - Warranties that the borrower will complete the plan;
  - Covenants ensuring that adequate resources are committed to complete the Year 2000 plan; and
  - Default provisions allowing the lender to accelerate the maturity of the debt for non -compliance with Year 2000 covenants;

- Credit Administration
  After the initial assessment, ongoing credit administration provides the best opportunity for an institution to manage Year 2000-related customer risk. Periodic credit analyses, which should include an update of the customer's Year 2000 efforts, can help to monitor a borrower's Year 2000 efforts. When performing credit analyses, loan officers should determine whether a customer's Year 2000-related risk merits an adjustment to its internal risk rating.

- ALLL Analysis
  Management's review of the adequacy of loan and lease loss allowances should include Year 2000 customer risk. When Year 2000 issues adversely impact a customer's creditworthiness, the allowance for loan and lease losses should be adjusted to reflect adequately the increased credit risk. Additionally, management's analysis of loss inherent in the entire portfolio should reflect Year 2000 risk.

Funds Providers
Management should consider the potential effect on an institution's liquidity by assessing the potential for unplanned reductions in the availability of funds from significant funding sources that have not taken appropriate measure to manage their own Year 2000 problems. Management should develop appropriate strategies and

contingency plans to deal with this potential problem.

- Risk Assessment of Funds Providers
  As with funds takers, management should discuss Year 2000 issues with significant funds providers, evaluate their Year 2000 readiness to the extent possible, and assess the Year 2000-related risks posed by the providers. Management should be aware of concentrations -- including concentrations in any single currency -- from an individual provider or group of providers that may not be Year 2000 ready.

- Contingency Planning
  The risk assessment of major funds providers' Year 2000 readiness should be incorporated into an institution's liquidity contingency plans. As with other contingency planning processes, management should evaluate its exposure and potential funds needs under several scenarios that incorporate different assumptions about the timing or magnitude of funds providers' Year 2000 -related problems. Institutions with significant funds flows in different currencies may needs separate contingency plans for each major currency.

  Although the liquidity risks from funds providers' Year 2000-related problems are similar to other "event risks" that institutions address in their liquidity contingency plans, Year 2000-related liquidity risks differ because the date of this event is known in advance. As a result, institutions may be better able to plan for and mitigate potential liquidity risks. For example, institutions may be able to reduce potential liquidity risks by extending the maturity of their advances under funding lines sufficiently past January 1, 2000, to provide time to assess and evaluate the effect of the Year 2000 on its funds providers. Maintaining close contact with funding sources throughout this potentially difficult period can provide management with timely, market sensitive information and thus allow for more effective liquidity planning.

Capital Market and Asset Management Counterparties
The focus of the controls for an institution's exposure to Year 2000-related problems in capital markets and among counterparties mirror those needed for funds takers and funds providers. Potential Year 2000-related problems with capital market participants range from a counterparty's failure to complete a securities transaction or derivatives contract settlement to, in extreme cases, the failure of the counterparty itself. A counterparty failure could lead to the total loss of the value of the payment or contract. A counterparty's failure to settle a transaction could cause the institution unexpected liquidity problems, which in turn could result in the failure of a financial

institution to deliver dollars or foreign currencies to its counterparties.

In addition, Year 2000-related problems among fiduciary counterparties could prevent a financial institution from fulfilling its fiduciary responsibilities to protect and manage assets for fiduciary beneficiaries. A counterparty's failure to remit bond payments, fund employer pension contributions or settle securities transactions could increase the institution's fiduciary risk.

- Risk Assessment of Counterparties
  As part of a sound due diligence process, management should identify and discuss Year 2000 compliance issues with those counterparties which represent large exposures to the bank itself and to fiduciary account beneficiaries. Financial institutions should evaluate counterparty exposure and develop risk reducing action plans to help manage and control that risk.

- Risk Reduction Plans
  In cases where institutions are not fully satisfied that their counterparties will be Year 2000 ready, management should establish mitigating controls such as early termination agreements, additional collateral, netting arrangements, and third-party payment arrangements or guarantees. In cases where management has a high degree of uncertainty regarding a counterparty's ability to address its Year 2000 problems, the institution should consider avoiding transactions with settlement risk after January 1, 2000. As noted earlier, the interest rate effect of material mismatches of funding, or maturity, should be evaluated as maturity and settlement risk is adjusted. The financial institution should not resume normal transaction activities until the counterparty has demonstrated that it will be prepared for the Year 2000.

## CONCLUSION

Financial institutions face significant internal and external challenges from Year 2000-related risks posed by their customers. The concepts and guidance in this interagency statement are designed to assist institutions in developing appropriate risk controls. The FFIEC recognizes that risk management procedures may vary depending on the institution's size, its risk appetite and culture, the complexity of its customers' information systems, and its own Year 2000 risk exposure. While these differences will affect the risk management practices developed by management, it is essential that financial institutions identify, measure, monitor and control Year 2000- related risks posed by funds providers, funds takers, and capital market/asset management counterparties.

Appendices (4)

# GUIDANCE
# CONCERNING INSTITUTION DUE DILIGENCE
# IN CONNECTION WITH
# SERVICE PROVIDER AND SOFTWARE VENDOR YEAR 2000
# READINESS

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

## Background

The Federal Financial Institutions Examination Council (FFIEC) has issued several statements on the Year 2000 problem. These interagency statements address key phases of the Year 2000 project management process and the specific responsibilities of senior management and the board of Directors to address business risks associated with the Year 2000 problem. Nearly all financial institutions in the United States rely on service providers and software vendors to operate mission-critical systems, and thus nearly all should work closely to ensure services and products are Year 2000 ready.

## Purpose

The purpose of this guidance is to ensure that senior management and the boards of Directors of financial institutions establish a due diligence process for determining the ability of its service providers and software vendors to become Year 2000 ready, establishing appropriate and effective remediation programs, establishing testing to the extent possible, and developing effective contingency plans in the event service providers and software vendors are not Year 2000 ready.

## Summary

Management of financial institutions should establish a comprehensive Year 2000 due diligence process with its service providers and software vendors. The due diligence process should enable management to:

Identify and assess the mission-critical services and products provided by service providers and software vendors;

- Identify and articulate the obligations of the service provider or software vendor and the institution for achieving Year 2000 readiness;
- Establish a process for testing remediated services and products in the institution's own environment to the extent possible;
- Adopt contingency plans for each mission-critical service and product; and
- Establish monitoring procedures to verify that the service provider or software vendor is taking appropriate action to achieve Year 2000 readiness.

## FFIEC Expectations and Efforts

In the May 1997 Interagency Statement, the FFIEC advised all financial institutions to identify service provider or software vendor interdependencies as part of its assessment phase. The FFIEC recommended that a Year 2000 readiness team and oversight committee, formed by the board of

Directors in consultation with senior management, be assigned the responsibility for identifying all systems, application software, and supporting equipment that are date dependent. Institutions should have completed their assessments by September 30, 1997. The Interagency Statement also addressed the importance of assessing mission-critical systems first because the failure of mission-critical services and products could have a significant adverse impact on the institution's operations and financial condition. Each system and application should be assessed based on the importance of the system and application to the institution's continuing operation and the costs and time required to implement alternative solutions.

The FFIEC recognizes that service providers and software vendors may not be able or may be unwilling to correct Year 2000-related problems for a variety of reasons. Developers of software and equipment may no longer be in business or they may no longer support the application or operating system. Source code may not be available for remediation and the systems and hardware equipment may have components that are no longer manufactured. In addition, a software provider that sells a large variety and volume of programs might provide only general instructions for reconfiguring a product to the user because of the high cost associated with changing each product. Alternately, a service provider may assume total responsibility for the renovation of its operating systems, software applications, and hardware because its systems are maintained internally. However, the FFIEC believes it is important that financial institutions obtain sufficient information to determine if their mission-critical service providers and software vendors will be able to successfully deliver Year 2000 ready products and services. This guidance assists financial institutions with managing their relationship with service providers and software vendors as their Year 2000 project management plan is implemented.

The FFIEC will support financial institutions in their efforts to meet the expectations addressed in this guidance. The FFIEC agencies will provide to the serviced institutions information on the level of preparedness of their service providers that the agencies inspect. In addition, the FFIEC agencies are encouraging software vendors to provide as much information as possible on their remediation and testing efforts to their client financial institutions. The FFIEC also plans to participate in industry-sponsored events to exchange information on software vendors and the due diligence process and post information on its Internet web site (www.ffiec.gov).

Due to the pivotal role played by service providers and software vendors in an institution's operations, the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the National Credit Union Administration have augmented their examination of service providers to include focused Year 2000 reviews. Although the agencies will not certify service providers or software vendors as Year 2000 compliant as a result of these reviews, the agencies will forward the results of service provider Year 2000 readiness examinations to the serviced institutions that use these service providers. The agencies also will examine software vendors that agree to periodic inspections. In those cases where the software vendor consents, the results of Year 2000 readiness examinations will be forwarded to client institutions.

The examination reports of service providers and software vendors should not be viewed as a substitute for independent due diligence of your service provider's and software vendor's Year 2000 readiness. The examination reports should not limit a financial institution's efforts to obtain information directly from the service provider and software vendors. The information contained in an examination report reflects the Year 2000 readiness of a service provider and software vendor as of a particular point in time. When reviewing these reports, institutions should be aware that circumstances may have changed since the review was conducted and follow up with the service provider and software vendor may be necessary.

Financial institutions may find it beneficial to join forces with other financial institutions in similar circumstances and coordinate group efforts to evaluate

the performance and testing methodologies of service providers and software vendors, to participate in testing efforts to the extent possible, and to evaluate contingency plans. By working through user groups, financial institutions can gather and disseminate information on the efforts of service providers and software vendors, testing methodologies, contingency plans and monitoring techniques. User groups also can be useful to encourage uncooperative service providers and software vendors to provide more prompt and effective service to client institutions.

**Responsibilities of Financial Institutions with Respect to Service Providers and Software Vendors**

The management of a financial institution is responsible for determining the ability of its service providers and software vendors to address Year 2000 readiness, for establishing appropriate and effective testing and remediation programs, and for developing effective contingency plans in the event providers are not Year 2000 ready. Financial institutions should contact service providers and software vendors to determine what is needed to make the product or service Year 2000 ready. Management also should assess whether the service provider or software vendor has the capacity and expertise to complete the task. Service providers and software vendors should make full and accurate disclosures to their client financial institutions concerning the state of their remediation efforts.

Management should request the following information for all mission-critical products provided by service providers and software vendors:

- Information on Year 2000 project plans, including the scope of the effort, a summary of resource commitments, dates when remediation and testing will begin and end, and dates when Year 2000 products and services will be delivered to the financial institution.
- Plans to discontinue or extensively modify existing services and products.
- Ongoing updates on the service providers' and software vendors' progress in meeting timetables of their Year 2000 project plans.
- Estimates of product and support costs to be incurred by the financial institutions required for remediation and testing.
- Contingency plans of service providers or software vendors in the event their project plans fail.

Financial institutions should thoroughly investigate the legal ramifications of renovating software vendor code because there is considerable legal risk in renovating software vendor-supplied code. For example, code modifications could render warranties and maintenance agreements null and void. However, financial institutions may need to make critical decisions that balance the consequences of these legal risks with business necessity. Financial institutions may also need to determine whether they can terminate their current service contracts and at what cost.

The failure of service providers and software vendors to meet these expectations could pose a risk to the safety and soundness of an institution and in such circumstances, institutions may need to terminate their relationship with the service provider or software vendor.

**Testing**

Testing for changes to the services and products will play a critical role in the Year 2000 process. Financial institutions should test, to the extent possible, service provider and software vendor provided products and services in the institution's own environment. The FFIEC expects service providers and software vendors to fully cooperate with financial institutions in testing. Management should not rely solely on the stated commitment of a service provider or software vendor to test but request that the scope be defined, objectives listed, and testing approaches and scenarios be developed. Testing schedules should be supplied by service providers and software vendors. In addition, the institution's testing strategy should include a testing scenario to simulate and measure the impact of a Year 2000-related disaster on normal operations.

The FFIEC will provide guidance on testing in an upcoming release.

**Contingency Plans**

Financial institutions should develop contingency plans for each mission-critical service and product. Contingency plans should describe how the financial institution will resume normal business operations if remediated systems do not perform as planned either before or after the century date change. They should establish "trigger dates" for changing service providers and software vendors to allow sufficient time to achieve Year 2000 readiness. Management of financial institutions, in consultation with the institution's legal counsel, should identify any legal remedies or resolutions available to the institution in the event products are not able to handle Year 2000 date processing. Institutions should consult with business partners that have interconnected systems, user groups, and third-party service providers.

If service providers and software vendors refuse or are unable to participate in Year 2000 readiness efforts or if commitments to migrate software or replace or repair equipment cannot be made by the "trigger date," the institution should pursue an alternate means of achieving Year 2000 readiness. In either of these cases, the institution should consider contracting with other service providers and software vendors to provide either remediation or replacement of a product or service. Difficulties of this nature should be reported to the financial institution's primary federal regulatory agency.

The FFIEC will provide detailed guidance on contingency planning in an upcoming release. However, that portion of a financial institution's Year 2000 contingency plan pertaining to service providers and software vendors should be tailored to the needs and complexity of the institution and should incorporate the following components:

- A risk assessment that identifies potential disruptions and the effects such disruptions will have on business operations should a service provider or software vendor be unable to operate in a Year 2000 compliant environment. The plan should determine the probability of occurrence and define controls to minimize, eliminate or respond to disruptions.
- An analysis of strategies and resources available to restore system or business operations.
- A recovery program that identifies participants (both external and internal) and the processes and equipment needed for the institution to function at an adequate level. The program should ensure that all participants are aware of their roles and are adequately trained.
- A comprehensive schedule of the remediation program of the service provider or software vendor that includes a trigger date. Institutions should assure themselves that adequate time is available should their internal test results require additional remediation efforts.

The development and implementation of contingency plans should be subject to the scrutiny of senior management and the board of Directors. Institution management should periodically review both its contingency and remediation plans. These reviews should address the impact that any changes made to a renovation plan might have on contingency plans. Additionally, the institution should ensure that an independent party review these plans. Finally, the institution's senior management and the board of Directors should review and approve all material changes to their plans.

**Monitor Service Provider and Software Vendor Performance**

Management of financial institutions should monitor the efforts of service providers and software vendors. The monitoring process should include frequent communication and documentation of all communication. Since the institution cannot rely solely on the proposed actions of service providers and software vendors, management should contact each mission-critical service provider and software vendor quarterly, at a minimum, to monitor its

progress during the remediation and testing phases. The institution should maintain documentation for all of its communications.

Many service providers and software vendors maintain web sites on the Internet with information about the Year 2000 readiness of their services and products. In addition, the FFIEC Year 2000 web site (www.ffiec.gov/Y2K/) includes links to other federal government web sites in which listings of various service provider and software vendor statements are maintained. To the extent that a financial institution relies on information from a web site, a paper copy of the information should be kept on file, and the web site periodically checked to determine if information has been updated.

**Conclusion**

The FFIEC expects management and the boards of Directors of financial institutions to establish a comprehensive Year 2000 due diligence process with its service providers and software vendors. Management of each financial institution is responsible for ensuring that its service providers and software vendors take adequate steps to address Year 2000 problems. Financial institutions should establish contingency plans to ensure that management has alternative options for all mission-critical systems in the event service providers and software vendors are not able to meet key target dates. Management should test services and products in the institution's own environment to the extent possible.