



RESCINDED

Office of Thrift Supervision
 Department of the Treasury
 200 Constitution Avenue, N.W., Washington, D.C. 20552 (202) 406-6800

Richard M. Riccobono
 Deputy Director

June 18, 1998

Any attachments to this document are rescinded only as they relate to national banks and federal savings associations.

MEMORANDUM FOR: Chief Executive Officers

FROM: Richard M. Riccobono *Richard M. Riccobono*

SUBJECT: FFIEC Guidance Concerning Contingency Planning and Customer Awareness

The OTS and the other FFIEC agencies recently issued guidance on contingency planning to mitigate risks due to the Year 2000 date change, and on responding to customer inquiries regarding Year 2000 concerns. This guidance follows previous FFIEC Year 2000 statements on project management, business risk, vendor management, corporate customers and testing. A copy of this guidance, which is also available on our web site (www.ots.treas.gov), is attached.

The purpose of the contingency planning guidance is to assist boards of directors and senior management in refining Year 2000 contingency plans. A business resumption contingency plan should provide assurance that mission-critical functions will continue if one or more systems fail. This plan should be reviewed, updated, and validated on a continuous basis. Ultimately, each institution's board of directors and senior management is responsible for the overall process and allocation of resources to ensure the success of the Year 2000 business resumption contingency plan.

This guidance addresses contingency planning with respect to renovation, testing plans, the continuation of automated information systems, and, most important, the continuation of all aspects of core business processes. The guidance outlines four phases of contingency planning. These phases are:

- Developing organizational planning guidelines for the institution to identify core business processes and prioritize business risks;
- Completing a business impact analysis on each core business process and defining and documenting Year 2000 failure scenarios;
- Preparing a contingency plan for each core process that identifies contingency options and implementation modes and establishing trigger dates to activate the contingency plan; and
- Validating the institution's contingency plans through an independent review of the feasibility of the plans and periodically testing the plans to ensure that changes in the institution's Year 2000 project plan and actual events are incorporated into the plans as appropriate.

The guidance on Year 2000 customer awareness provides suggestions for developing a customer awareness program. It identifies issues that institutions should be prepared to discuss with customers. A proactive approach to addressing customer concerns is critical to maintaining public confidence in the financial system. Examiners will be reviewing the adequacy of your institution's customer awareness strategy. In developing a program, consider some of the issues customers may be interested in discussing, and communicate with them about what could happen and what they should do if problems do arise. Some potential customer inquiries include concerns about:

- The safety of the money in their accounts;
- Access to their funds, such as access through ATMs, debit cards, telephone lines or the Internet, and the arrangements the financial institution will make to ensure alternative means of access to funds if disruptions occur;
- Availability of information on or summaries of the financial institution's Year 2000 project management and contingency plans; and
- Whether direct deposit, direct debit and other automatic electronic payments will be made on a timely basis and credited or debited accurately to the proper accounts, and what arrangements the institution will make to deal with such transactions should disruptions occur.

The FFIEC is developing a brochure that provides consumer information about the Year 2000 challenge. The brochure will be mailed to insured financial institutions by the FDIC in the next few weeks. It will explain the steps financial institutions and the federal financial institution regulators are taking to address the date change problem and emphasizes that it will not affect deposit insurance coverage. You may wish to order multiple copies and distribute the brochure as part of your communications with customers.

We are interested in your questions and concerns regarding efforts to make your systems ready for the Year 2000 date change. Please contact the Year 2000 Coordinator at your regional OTS office; Dorothy Van Cleave, National Year 2000 Coordinator at (202) 906-7380; or Jennifer Dickerson, Manager, Information Systems Examinations at (202) 906-5631 for further assistance.

Attachments



May 13, 1998

GUIDANCE CONCERNING CONTINGENCY PLANNING IN CONNECTION WITH YEAR 2000 READINESS

To: The Board of Directors and Chief Executive Officers 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) issued an interagency statement May 5, 1997, entitled "Year 2000 Project Management Awareness," that provided guidance for insured financial institutions to manage the phases of their Year 2000 readiness program. Subsequently, the FFIEC issued four statements that provided additional guidance on key issues including business risk, vendor due diligence, customer risk, and testing. Accordingly, financial institutions should be well into their Year 2000 readiness plan. The Awareness and Assessment phases should be completed. The Renovation and Validation Phases are current priorities and should be in process.

Another essential component of preparing for the Year 2000 problem¹ and beyond is developing options for the board of directors and senior management if any or all of the financial institution's systems fail or cannot be made Year 2000 ready. The interagency statement "Guidance Concerning Institution Due Diligence in Connection with Service Provider and Software Vendor Year 2000 Readiness," issued March 17, 1998, recommended that financial institutions adopt contingency plans for their mission-critical services and products. That issuance also provided guidance for developing contingency plans designed for external providers. The FFIEC has also issued previous guidance on contingency

¹ Any problem which prevents information technology from accurately processing, calculating, comparing, or sequencing date or time data from, into, or between the 20th and 21st centuries; or the years 1999 and 2000, or with regard to leap year calculations.

planning.²

The guidance provided in this paper is modeled after the United States General Accounting Office exposure draft "Year 2000 Computing Crisis: Business Continuity and Contingency Planning," released in March 1998 (GAO/AIMD-10.1.19 at www.gao.gov).

Purpose

The purpose of this guidance is to assist the board of directors and senior management of financial institutions as they refine the Year 2000 contingency plans developed during the assessment phase. A financial institution should design its Year 2000 contingency plan to mitigate the risks associated with (1) the failure to successfully complete renovation, validation, or implementation of its Year 2000 readiness plan (Remediation Contingency Plan), and (2) the failure of systems at critical dates (Business Resumption Contingency Planning). While Remediation Contingency Planning has been addressed in previous FFIEC guidances, the last section of this paper provides clarification of certain aspects of that guidance. The primary subject of this paper, however, is Business Resumption Contingency Planning.

Summary

The FFIEC recognizes that each financial institution operates with a unique aggregation of technological resources within the confines of a predefined operating structure. Thus, there are no ideal or simple solutions to Year 2000 contingency planning. This policy statement presents guidance and recommendations, but is not intended to be an all-inclusive Year 2000 contingency planning solution. Each financial institution must evaluate its own unique circumstances and environment to develop a comprehensive plan to ensure its ability to continue as a functioning business entity after January 1, 2000. The board of directors and senior management should attach a high priority to the development, validation, and implementation of the Year 2000 contingency plan.

² On March 26, 1997, the FFIEC issued a policy statement entitled "Corporate Business Resumption and Contingency Planning." Although not specific to the Year 2000 readiness issue, the statement emphasized the importance of the business resumption and information systems contingency planning functions, including planning for critical information systems and operations supported by service providers. Financial institutions were encouraged to ensure that contingency plans were comprehensive and thoroughly tested. (This paper can be obtained at <http://www.fdic.gov/banknews/files/1997/fil9768.html>).

To produce a viable Year 2000 business resumption contingency plan in a cost effective manner, each financial institution should evaluate the risks associated with the failure of core business processes. Core business functions or processes of a financial institution are groups of related tasks that must be performed together to ensure that the financial institution continues to be viable. Evaluation of these risks should include comparing the cost, time, and resources needed to implement the contingency alternatives.

BUSINESS RESUMPTION CONTINGENCY PLANS

Financial institutions' boards of directors and senior management should ensure that their institutions' Year 2000 contingency planning process encompasses a plan of action in the event that there are systems failures at critical dates. The business resumption contingency planning should be incorporated into the institutions' overall Year 2000 contingency plan.

The four phases of the Year 2000 business resumption contingency planning process should include:

1. Establishing *Organizational Planning Guidelines* that define the business continuity planning strategy;
2. Completing a *Business Impact Analysis* where the financial institution assesses the potential impact of mission-critical system failures;
3. Developing a *Contingency Plan* that establishes a timeline for implementation and action, circumstances, and trigger dates for activation; and
4. Designing a method of *Validation* so that the business resumption contingency plan can be tested for viability.

The phases of the process are more fully discussed below.

Examiners from the FFIEC member agencies will address the Year 2000 business resumption contingency planning process as part of each financial institution's Year 2000 readiness examination.

Attaining Year 2000 readiness is one of the most complex and challenging issues facing a

financial institution's board of directors and senior management. Many financial institutions will expend substantial resources to renovate or replace mission-critical systems, yet despite this effort and commitment, the risk of disruption to business processes remains. A Year 2000 business resumption contingency plan should be designed to provide assurance that the mission-critical functions will continue if one or more systems fail. Furthermore, it should not be viewed as a static document, but as a process that should be reviewed, updated, and validated on a continuous basis.

Organizational Planning

The board of directors and senior management must be directly involved in the financial institution's Year 2000 business resumption contingency planning process. The production of the contingency plan document may be delegated to staff and implementation decentralized to segments of the financial institution's operations. Ultimately the board of directors and senior management are responsible for the overall process and assure that sufficient resources are made available to ensure the success of the Year 2000 business resumption contingency plan.

Establishment of a continuity project work group and assignment of roles and responsibilities.

Depending on the size and complexity of the financial institution, this may be an individual; or representatives from all major business segments, including disaster recovery specialists, and audit representatives, if available. This individual or group will develop the continuity plan and later develop and monitor the Year 2000 business resumption contingency plan.

Identification of core business processes.

Mission-critical systems were identified during the assessment phase. Core business processes that utilize these mission-critical systems may have also been identified. Beyond the information system relationships, all aspects of the business process should now be defined.

It is important to ensure that key internal and external business dependencies are identified, including infrastructure and information sources. While the financial institution may have only limited control of the impact of these elements on the operations, it is essential that the institution identify these elements in order to establish contingency alternatives.

Establishment of an event timeline.

Each financial institution should develop a timeline of events that incorporates the schedule of renovation and testing in the financial institution's Year 2000 readiness plan. The Year 2000 business resumption contingency plan should specifically identify a pre-Year 2000 event³ timeline as well as a post-Year 2000 event timeline. Critical stages must be identified, assessed for feasibility of implementation, and updated as necessary.

Development of a risk management process and reporting system.

Business risks should be prioritized with the business resumption contingency planning efforts focused on the core business processes that, should they be compromised, pose the greatest risk to the institution. Year 2000 readiness risks should be identified and a system developed that provides an adequate means of reporting progress and changes in the Year 2000 readiness plan.

Review of existing business continuity or contingency plans and disaster recovery programs.

The financial institution should assess the strengths and weaknesses of these programs to determine their continued effectiveness and to eliminate redundancy and any waste of resources. For example, a financial institution may consider using an existing contract for a hot-site that will process mission-critical information systems in the event of a disaster.

Business Impact Analysis

This phase assesses the potential impact of mission-critical system failures on the core business processes. The financial institution should assign priority to the business processes. The results of this analysis provides the basis for the contingency plan.

Perform a risk analysis of each core business process.

Issues to be considered may include:

- The status of Year 2000 readiness renovation or replacement plans for mission-critical systems, whether administered internally or by service providers;

³ The system may fail because a date past December 31, 1999, such as a loan due date is input or computed and then rejected.

- The financial and marketing impact of the loss of a core business process, including what impact the loss might have on the viability of the financial institution; and
- The impact of regulatory requirements.

Define and document Year 2000 failure scenarios. Consider the risk of both internal and infrastructure failures.

The results of tests run on renovated systems may lead to the development of the failure scenarios. For example, an ATM network failure may necessitate increased teller staff to accommodate increased lobby traffic.

Determine the minimum acceptable level of outputs and services.

For example, those responsible should establish the minimum frequency for production of demand deposit, savings, and loan trial balances.

Year 2000 Business Resumption Contingency Planning

The financial institution should now develop its Year 2000 business resumption contingency plan based on the priorities established during the business impact analysis. The plan should be documented and organized so that it can be easily changed if necessary.

Evaluate options and select the most reasonable contingency strategy.

The strategy should be cost-effective, practical and appropriate for the size, complexity, and type of information systems used. In selecting a strategy, consider the cost and functionality of the strategy and the feasibility of deploying the event timeline. The primary goal should be to maximize the functionality and speed of recovery. Financial institutions serviced by third-parties should develop strategies that take into account the contingency alternatives outlined in those third-party contingency plans.

Identify contingency plans and implementation modes.

Develop a specific recovery plan for each core business process that considers the minimum level of acceptable output. Evaluate the need for specific strategies such as quick fixes, partial replacement outsourcing or other alternatives. The plan could include consideration of whether the systems to support the core business processes could be replaced by manual or automated processes.

Document the products of the core business processes that may need to be recovered. Each financial institution should review its Year 2000 readiness plan to determine the key dates that tie to this data. In general, the following items should be included:

- Machine-readable copies of the institution's master-files and transaction files;
- Printed (or other similar medium such as microfiche) trial balances;
- A master list of Year 2000 readiness contact points of every client, supplier, bank, and government agency that shares data with the institution;
- Electronic text-format copies of all master files and trial balance reports; and
- In those instances where the financial institution's data processing facility is providing services to other financial institutions, a copy of machine-readable data files, for all customers.

Other important review processes to consider include:

- Legal counsel reviews of data processing and service providers' contracts where necessary to determine the responsibilities of each of the parties;
- Comprehensive review of all of data processing insurance coverage;
- Public relations responsibilities that are organized and delegated to specific individuals or committees ensuring that appropriate staff make accurate statements;
- Review of all Local Area Network (LAN) and Wide Area Network (WAN) access to other systems; and
- Review and testing the financial institution's disaster recovery site to ensure that Year 2000 capable hardware is available if needed.

Establish trigger dates to activate the contingency plans.

Those responsible for the plan should continuously evaluate the progress of the Year 2000 readiness plan and report any deviation from the plan to senior management. They should monitor critical milestones and establish trigger dates for implementation of the contingency plans. Those trigger dates should take into account what would be involved in obtaining alternative sources of service.

Assign responsibility for business resumption of core business processes.

Either an individual or team should be responsible for managing the implementation of the contingency plan.

Implement an independent review of the feasibility of the contingency plan.

Who conducts the review will depend on the size and complexity of the financial institution. The party responsible should be independent of the contingency plan process.

Develop an implementation strategy for the physical rollover.

Management should ensure that there are plans in place and staff available for the period December 30, 1999, and January 3, 2000, and the other key milestone dates.

Validation of the Business Resumption Contingency Plan

Throughout this document, contingency planning has been referred to as a process. Modifications or corrections to the financial institution's Year 2000 readiness plan may prompt modifications or corrections to the contingency plan. Periodic tests of the contingency plan will ensure that these changes are considered and that the level of support for the core business processes is adequate. The frequency and sophistication of testing should be consistent with the size and complexity of the financial institution.

Financial institutions should develop and document business resumption contingency test plans approved by senior management. The test plans should be independently validated in order to judge the effectiveness and reasonableness of the proposed contingency plan. This independent validation should be performed by knowledgeable individuals who were not involved in the formulation of the plans. If the financial institution does not have the expertise in-house, they should secure the expertise from other sources. Based on those test results, modifications should be made to ensure that the business continuity plan remains valid.

REMEDIATION CONTINGENCY PLANS

Thus far, guidance in this paper has addressed the planning efforts needed to mitigate the operational risks should systems fail at critical dates. Other key aspects of the broader contingency planning concept have been discussed in previous FFIEC guidance papers related to the Year 2000 computer problem. These aspects included planning that mitigates the risks associated with the failure to successfully complete renovation, validation and implementation of mission-critical systems. This facet of contingency planning is referred to as remediation contingency planning and pertains to mission-critical systems developed in-house, by third party service providers, and by software vendors. The following guidance is intended to clarify supervisory expectations as outlined in the Interagency Statement issued May 5, 1997, "Year 2000 Project Management Awareness."

If a mission-critical application or system has been remediated, tested and implemented, a remediation contingency plan is not required. If internal remediation efforts or vendors are expected to provide Year 2000 ready products and services within a short period of time (no later than July 31, 1998), remediation contingency plans may not be necessary for those systems. However, the financial institution should establish a firm date that would trigger completion of the remediation contingency plan should internal efforts or the efforts of the institution's vendor or servicer fail to provide a Year 2000 ready product or service.

If a system is in the process of remediation, and is on schedule to meet FFIEC timeframes, comprehensive remediation contingency plans may not be necessary. At a minimum, financial institutions should develop remediation contingency plans which (1) outline the alternatives available if remediation efforts are not successful, (2) consider the availability of alternative service providers or software vendors, and (3) establish trigger dates for activating the remediation contingency plan, taking into account the time necessary to convert to alternate service providers or software vendors.

The FFIEC understands that ensuring the availability of an alternative servicer or vendor may require payment of a fee. Whether or not to pay this fee is a business decision that the financial institution board of directors and senior management must make. The decision should consider the probability of failure of the institution's internal efforts, or the remediation efforts of existing service providers or software vendors. Management should also consider the following:

- The extent to which the existing service provider or software vendor has met milestones established by the financial institution;

- The amount of time necessary to migrate to an alternate service provider or software vendor;
- The availability of alternative service providers or software vendors; and
- Any information about the alternate service provider or software vendor available from user groups or others.

Conclusion

The FFIEC realizes that the complexity of a financial institution's Year 2000 business resumption contingency plan will vary depending upon the complexity of its information system structure; however, the FFIEC expects financial institutions to develop, implement, and validate Year 2000 contingency plans designed to mitigate the risks associated with the Year 2000 date change. The Year 2000 contingency plan should be in writing and documented to support the conclusions and procedures therein. The board of directors and senior management are responsible for ensuring that the Year 2000 contingency plan is comprehensive and adapted for the unique attributes of their financial institution.



May 13, 1998

Guidance on Year 2000 Customer Awareness Programs

To: The Board of Directors and Chief Executive Officer of all federally supervised financial institutions, 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 project management phases, specific responsibilities of the board of directors and senior management with respect to business risks, due diligence with respect to service providers and software vendors, risks associated with financial institution customers, and testing for Year 2000 readiness.

On December 17, 1997 the FFIEC issued business risk guidelines which required institutions to develop strategies for responding to inquiries from customers and business partners regarding the institution's Year 2000 readiness. Financial institutions have a responsibility to provide forthright and honest responses to questions and concerns that customers and business partners may have concerning their financial institution's Year 2000 readiness. The scope of this guidance is customer awareness (in contrast to business partner) policies. Institutions should consider including the components described below in their customer awareness programs, as appropriate.

Purpose

Customers of financial institutions will look to institutions for assurances that the institution is taking appropriate steps in preparation for the century date change. This statement provides suggestions for developing a customer awareness program and identifies issues that financial institutions should be prepared to discuss with customers.

Awareness Program for Customers

The regulators expect financial institutions to develop a customer awareness program which responds to questions and communicates with customers on Year 2000 matters. During on-site Year 2000 examinations, examiners will be reviewing the adequacy of an institution's customer awareness strategy. Effectively responding to customer inquiries also is in the best interests of the financial institution. It can serve to disclose to customers the institution's Year 2000 efforts and to provide information on how products and services used by those customers may be affected by the institution's readiness efforts. Ultimately, achieving Year 2000 readiness and ensuring that customers and business partners receive adequate information about an institution's efforts is and must be the responsibility of a financial institution's directors and officers. Management is in the best position to know how the Year 2000 date change will affect an institution's operations, strategies, resources and exposures, and how and when it would be best to respond to the specific concerns of its customers.

The FFIEC agencies are encouraging customers with questions and concerns about Year 2000 readiness to contact their financial institutions directly. Financial institutions are of different sizes, offer different ranges of products, and vary in the complexity of information systems. This guidance recognizes these differences and provides the following suggestions that can be used to develop a program to respond to customer inquiries about the Year 2000 problem.

In developing a customer awareness strategy, financial institutions should identify those customers who should be proactively informed of efforts to address business risks arising from the Year 2000 problem. Customers may include depositors, borrowers, fiduciary clients, or others who engage in transactions with the institution. Next, financial institutions should consider the most effective ways of communicating with various types of customers about the status of the financial institution's Year 2000 readiness. Depending upon the institution's size and business environment, possible methods include:

- Providing informational brochures or other written disclosures in monthly or quarterly statements;
- Establishing toll-free hotlines for customer inquiries;
- Holding seminars to discuss the Year 2000 problem and efforts the financial institution is taking to prepare for the century date change; and
- Developing Internet sites—or perhaps an exclusive portion of their existing site—to inform customers of their Year 2000 preparedness efforts.

It is recommended that financial institutions consult with legal counsel before issuing

information describing the status of Year 2000 readiness efforts.

The customer awareness program should ensure that personnel who regularly interact with customers are trained to respond appropriately to inquiries by referring customers to appropriate explanatory materials or expert financial institution staff. Institutions also may consider including interested external parties (such as the news media and community organizations in the financial institution's service area) in the communication program, as appropriate.

In developing customer awareness programs, financial institutions should consider some of the issues customers may be interested in discussing and effectively communicate with them about what could happen and what they should do if problems do arise. Some potential customer inquiries include concerns about:

- The safety of the money in their accounts.
- Access to their funds, such as access through ATMs, debit cards, telephone lines or the Internet, and the arrangements the financial institution will make to ensure alternative means of access to funds if disruptions occur.
- Whether they should withdraw some cash from their accounts prior to December 31, 1999.
- Availability of information on or summaries of the financial institution's Year 2000 project management and contingency plans.
- Whether direct deposit, direct debit and other automatic electronic payments will be made on a timely basis and credited or debited accurately to the proper accounts, and what arrangements the institution will make to deal with such transactions should disruptions occur.
- How the financial institution will assist any customers who may be affected by incorrect automatic transactions such as direct deposit and direct debit initiated by the institution or by third parties.
- Whether customers might not receive proper credit for loan payments.
- The financial institution's record keeping practices.
- The types of records customers should maintain prior to and after January 1, 2000.

The FFIEC is developing a consumer brochure that provides information to consumers

about the Year 2000 challenge. The brochure will explain the steps financial institutions and the federal financial institution regulators are taking to address the century date change and emphasizes that the Year 2000 date change will not affect deposit insurance coverage. Financial institutions may wish to use the brochure as part of their communications with customers. The brochure will be available by June 1998. The federal financial institution regulatory agencies will supply each institution with one copy of the brochure along with instructions for ordering multiple copies, should institutions wish to provide them to their customers.

Depository institutions are reminded that they may not disclose publicly the contents of federal supervisory agency examination reports or reviews of the institution or any service provider or software vendor, including the confidential Year 2000 summary ratings contained therein. Thus, in designing their Year 2000 public awareness plans and efforts, institutions should be careful not to violate this prohibition. Moreover, they should avoid any statements that indicate or imply that the institution's readiness has been approved or certified by a supervising agency with regard to its Year 2000 plan.

Conclusion

Financial institutions should develop a pragmatic strategy for responding to customer inquiries about their institution's Year 2000 readiness. The guidance in this interagency statement is designed to assist financial institutions in developing their programs. Each institution may choose to tailor its customer awareness program based on its own business environment, but ultimately, it is essential that each institution develop a program to address customer questions and concerns about the status of Year 2000 readiness.