ירושלים, ל' סיון, תשנ"ח
24 יוני, 1998
חוזר מס' ח- 06 - 1927

לכבוד
התאגידים הבנקאיים

הנדון: **שנת 2000 - הערכות המערכת הבנקאית**

מבוא

1. בהמשך למכתבים ולחוזרים הקודמים בקשר להערכות המערכת הבנקאית לשנת 2000, להלן דגשים נוספים המתייחסים לשלבי ההערכות המתקדמים - הניסויים לסוגיהם, וכן הכנת תוכניות חלופיות להתמודדות עם תקלות ועיכובים בתהליך ההערכות עצמו, או בתפקוד מערכות קריטיות מסויימות לאחר מכן.

תכנון וביצוע ניסויי המערכות

2. (א) ככל שהתקדם הטיפול בהערכות לשנת 2000, התחזקה ההכרה בחשיבות תכנון וביצוע ניסויי המערכות; מורכבות ניסויי המערכות מצריכה משאבי זמן, כח אדם ועלויות המוערכות ביותר מ- 50% מכלל ההקצאה לפרוייקט. תכנון, ניהול וביצוע נכון של הניסויים, ובפרט ניסויי ה-Ageing, על פי לוח זמנים קפדני, הינם קריטיים להצלחת ההיערכות בכללותה. תשומת לב מיוחדת יש לתת גם לתכנון הניסויים של המימשקים עם גורמי חוץ שונים (רשויות, בורסה, לקוחות וכד').

(ב) תאגידים בנקאיים שטרם הביאו לעיון הדירקטוריון את עיקרי תוכניות הניסוי שלהם מתבקשים לעשות כן לא יאוחר מהדיווח החודשי לדירקטוריון ל- 30.9.1998.
לנוחותכם, רצ"ב מסמך של ה-
Federal Financial Institutions Examination Council (FFIEC) של ארה"ב, בו מוצגים עקרונות והיבטים חשובים במתווה ניסויי ההערכות לשנת 2000 (נספח 1).

תכניות חלופיות למקרה של תקלות בהערכות (Contingency Planning)

3. (א) במקביל למאמצים המוקדשים להערכות נאותה לשנת 2000, יש לגבש תכניות חלופיות במטרה להתמודד עם עיכובים ותקלות בתהליך ההסבה, ולמזער את הסיכונים והנזק מתקלות במערכות קריטיות אם יתברר שהסבתן לא צלחה.
יש לגבש ולהביא לאישור הדירקטוריון תוכנית כוללת בנושא זה, לא יאוחר מ- 30.9.1998.

(ב) להלן מספר היבטים אליהם יש להתייחס בהתווית התוכניות בנושא:

(1) יש לקבוע את הגורם האחראי על התכנית - גיבושה ועידכונה השוטף (שינויים מהותיים יש להביא לאישור הדירקטוריון).

(2) התוכניות תכלולנה:

(א) הגדרת תרחישי "חרום" לעניין הפעלת האמצעים החלופיים;

(ב) עבור כל אחד מהתרחישים - דרכי הפעולה לפתרון הבעיה ולמיזעור נזקיה;

(ג) התכנית תתייחס לכל המערכות הקריטיות (בסיסי מידע, תוכנות, מערכות הפעלה, חומרה וציוד, תשתיות, מימשקים עם גורמי חוץ וכד');

רצ"ב לנוחותכם מסמך נוסף של ה- FFIEC בנושא זה (נספח 2).

ביטוח

4. יש לבדוק את פוליסות הביטוח של הבנק ואת ההסכמים עם הספקים וגורמי חוץ אחרים, הקשורים עם הבנק, בהתייחס לנזקים שעלולים להגרם לבנק עקב חוסר התאמה של מערכותיהם.

דיווח לפיקוח על הבנקים

5. תאגיד בנקאי ישלח למחלקת הפיקוח על הבנקים את הדיווחים הבאים:

(א) עותק מהדיווח לדירקטוריון כאמור בסעיף 2(ב) (עיקרי תכניות הניסוי) וזאת לא יאוחר מ- 15.10.1998.

(ב) על התאגיד הבנקאי לדווח מיידית על כל כשלון מהותי של שלב או סוג ניסוי, או של ניסוי מערכת קריטית.לעניין זה, כשלון מהותי הוא כזה שהתיקון והניסוי מחדש צפויים להמשך יותר משלושה שבועות.

(ג) תכנית חלופית למקרה של תקלות בהערכות, כמפורט בסעיף 3(א), וזאת לא יאוחר מ- 15.10.1998.

(ד) הודעה מיידית על התממשות תרחיש "חרום" כאמור בסעיף 3(ב)(2)(א).

6. הדיווחים יישלחו למר יצחק כהן ביחידת מידע ודיווח במחלקת הפיקוח על הבנקים ירושלים.
כמו כן, בדבר שאלות ובירורים ניתן לפנות למר דניאל מאיר במשרדנו בתל אביב בטלפון: 03-5640546.

בכבוד רב,

זאב אבלס

המפקח על הבנקים

(docs 7643)

Interagency Statement
April 10, 1998 statement

Guidance Concerning Testing for Year 2000 Readiness

To: The Board of Directors and Chief Executive Officers of all federally supervised financial institutions, examining personnel and senior management of each FFIEC agency, and all service providers and software vendors who provide services or software to federally supervised financial institutions.

BACKGROUND:

The Federal Financial Institutions Examination Council (FFIEC) has issued several statements on the Year 2000 problem. These interagency statements address key phases in the Year 2000 process, specific responsibilities of the board of directors and senior management with regard to the business risks, the due diligence process in connection with service providers and software vendors, and risks associated with financial institution customers. The FFIEC considers testing to be the most critical phase of the Year 2000 readiness process. Failure to conduct thorough testing may mask serious remediation problems. Failure to properly identify or correct those problems could threaten the safety and soundness of the institution.

PURPOSE:

The purpose of this guidance is to describe FFIEC expectations regarding the Year 2000 testing efforts of financial institutions. This guidance identifies key milestones and testing methods for financial institutions to use to prepare their systems and applications for the Year 2000.

SUMMARY:

Each financial institution is unique and management should determine the best testing strategies and plans for its organization taking into account the size of the institution, the complexity of its operation, and the level of its own business risk exposure to the Year 2000. Ultimately, each financial institution is responsible for ensuring its readiness for the Year 2000. The FFIEC expects financial institutions to meet key milestones in their Year 2000 testing process. Financial institutions should develop and implement a written testing strategy and plan to test both internal and external systems (including hardware, software, and environmental systems). Financial institutions should test mission-critical systems first [1]. The plans should include, at a minimum, the following elements: testing environment, testing methodology, testing schedules, human and financial resources, critical test dates, documentation, and contingency planning. Management should ensure that qualified sources verify the testing process.

KEY MILESTONES FOR TESTING PHASE

The FFIEC expects financial institutions to meet the following key milestones in their Year 2000 testing process. On or before:

June 30, 1998	Institutions should complete the development of their written testing strategies and plans.
September 1,1998	Institutions processing in-house and service providers should have commenced testing of internal mission-critical systems, including those programmed in-house and those purchased from software vendors.
December 31, 1998	Testing of internal mission-critical systems should be substantially complete. Service providers should be ready to test with customers.
March 31, 1999	Testing by institutions relying on service providers for mission-critical systems should be substantially complete. External testing with material other third parties (customers, other financial institutions, business partners, payment system providers, etc.) should have begun.
June 30, 1999	Testing of mission-critical systems should be complete and implementation should be substantially complete.

TESTING FOR YEAR 2000 READINESS

The FFIEC estimates that testing will consume 50 to 60 percent of the time, funding, and personnel needed to make financial institutions Year 2000 ready. Testing is critical to ensure that remediation efforts work effectively. Financial institutions must test because of the widespread changes being required to become Year 2000 ready. The software and hardware changes may not affect only one isolated application or system, but they may affect many or all internal systems and interfaces with internal and external entities.

The FFIEC expects financial institutions to manage effectively the Year 2000 testing process, regardless of how individual systems are developed and operated. In practice, the controls necessary to manage the testing process effectively will differ depending on the design of the financial institution's system, interfaces with third parties, and the type of testing used. Management is responsible for ensuring that testing is conducted by the party in the best position to perform the testing and assess the results.

Given the size and complexity of an institution and its testing needs, the FFIEC recognizes that the testing process may present a myriad of problems to financial institutions that program systems "in-house" as well as financial institutions that rely on service providers and software vendors. Some of these problems may involve only the coordination of available resources and timing, while others may entail more fundamental issues regarding a financial institution's ability to remediate all systems successfully by the Year 2000.

Financial institutions should test mission- critical systems first, as the failure of mission-critical services and products will have a significant adverse impact on the institution's operations and financial condition. Each system and application should be evaluated and tested based on its importance to the institution's continuing operations and the costs and time required to implement alternative solutions.

The FFIEC expects financial institutions to obtain sufficient information to determine if their mission-critical service providers and software vendors are able to test successfully products and services to ensure that service providers and software vendors are Year 2000 ready. The failure of these service providers and software vendors to test adequately their products and services could pose a risk to the safety and soundness of financial institutions.

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. Such user groups also can be beneficial to financial institutions as a forum to exchange ideas and information on testing within the institution's own environment.

The extent to which financial institutions rely on third parties to design, implement and manage their systems will affect the extent of an institution's involvement in testing. Financial institutions that outsource all of these functions will have less extensive involvement in testing than financial institutions that perform some or all of their own programming or processing in-house.

Testing Methodologies

The FFIEC recognizes that there is no single approach to testing for the Year 2000. Testing options range from testing within a financial institution's own environment to proxy testing. Where, how, and when testing is conducted will depend on a variety of factors, including whether the testing is being conducted on software or services received from third parties, as well as the type of system or application to be tested.

Listed below are representative types of tests that financial institutions could use in validating their systems. The terminology to describe these tests may vary among financial institutions. Each financial institution should determine the types of tests it will perform based on the complexity of its systems, the level of its Year 2000 risk exposure and its reliance on third parties for computer-based products and services. Moreover, in addition to testing a particular product or service, financial institutions should conduct testing between systems and products that interface with internal and external entities. The following are examples of various types of tests.

> *Baseline* tests are performed before any changes are made to a computer program or application. The baseline test helps a financial institution compare performance of the system after changes are made to it.
>
> *Unit tests* are performed on one application to confirm whether remediation efforts yield accurate results for that application. They do not test how well the application will perform with other applications.
>
> *Integrated tests* are performed on multiple applications or systems simultaneously. Integrated tests confirm whether computer programs function properly as they interact with other programs.

Regression tests verify a remediated system against the original system to ensure that errors were not introduced during the remediation process. Regression testing should be applied to both the remediated portion and the unchanged portion of the system.

Future date tests simulate processing of renovated programs and applications for future critical dates to ensure that those dates will not cause program or system problems.

User acceptance tests are performed with users and validate whether the remediations have been done correctly and applications still function as expected.

Point-to-point tests verify the ability of a financial institution to transmit data directly to another entity or system.

End-to-end tests verify the ability of a financial institution originating a transaction to transmit test data to a receiving entity or system through an intermediary.

Written Testing Strategy and Plan

Financial institutions should develop a testing strategy and set testing priorities based on the risks that the failure of a system may have on operations. The objective of a financial institution's Year 2000 testing strategy is to minimize business risk due to operational failures.

Financial institutions should develop a written testing plan to implement the testing strategy. The plan should provide for testing of both internal and external systems. Internal systems may include software, operating systems, mainframe computers, personal computers, reader/sorters, and proof machines. Internal systems also may include environmental systems including heating and cooling systems, vaults, security systems, and elevators. External systems may include services from service providers and any interfaces with external entities.

Management and staff are expected to have the knowledge and skills necessary to understand and effectively manage their Year 2000 testing efforts. Management should identify special staffing and training needs for personnel involved in testing. They also should determine how they will allocate resources and, if necessary, hire and train employees to run and analyze tests. Examiners will evaluate testing efforts by reviewing a financial institution's testing strategies and testing plans to ensure that it can meet key milestones addressed in this guidance.

Elements of a Testing Plan

Financial institutions should develop and implement a testing plan that includes the following elements. These elements apply to financial institutions that test systems programmed in-house, as well as financial institutions that test with service providers and software vendors.

Testing Environment. Considerations for an appropriate test environment should include whether to partition current operating computers, by setting aside one or more sections to be used only for testing, or by using a separate computer system to test. Testing should not be done in a production environment. If the institution uses either a separate computer facility or the computer at its contingency site, it should consider how all interfaces, both internal and external, will be duplicated and adequately tested. Management should evaluate whether the test environment has sufficient computing capacity needed to complete the testing plan.

Testing Methodology. The plan should address the types of tests for each application and system. See "Testing Methodologies" above for a description of various tests.

Test schedules. The plan should identify when software and hardware will be tested, including interfaces between systems. Test schedules also should be coordinated with the test schedules of third parties.

Human and financial resources. The plan should include budget issues as well as a description of the participants to be involved in testing, (e.g., the information technology staff, end-user, and external parties).

Critical Test Dates. Financial institutions should determine critical dates to be tested for each of their mission-critical systems. If an institution's systems or applications fail to operate properly when tested for these critical dates, management must determine whether remediation and subsequent testing can be completed successfully or whether contingency plans must be implemented. Critical dates may vary for a variety of reasons. Because additional dates may be critical for a given financial institution, each institution should test of the dates it deems critical. Financial institutions should test for any of the following dates that are applicable, including the "rollover" or progression before and after these dates, to ensure that applications and systems will operate properly:

Date	Reason
April 9, 1999	9999 on the Julian Calendar.[2] The 99th day of the year 1999. 9999 denotes the "end of input" in many computer programs.
September 9, 1999	9999 on the Gregorian Calendar. 9999 denotes the "end of input" in many computer programs.
December 31, 1999	Last day in 1999 year.
January 1, 2000	Beginning of the Year 2000
January 3, 2000	First business day in the Year 2000
January 10, 2000	First date to require a 7 digit date field (1/10/2000).

January 31, 2000	End of the first month of the year 2000
February 29, 2000	Leap year day.
March 31, 2000	End of first quarter of 2000.
October 10, 2000	First date to require an 8 digit date field (10/10/2000)
December 31, 2000	End of Year 2000
January 1, 2001	Beginning of the Year 2001
December 31, 2001	Check that year has 365 days.

Documentation. The institution should maintain written documentation supporting every stage of the testing process. This documentation provides an audit trail and should facilitate corrections of problems when they occur. The documentation should include the following:

Types of tests performed (e.g. baseline, unit, regression, etc.);

Explanation of why an institution chose the tests that it performed and how extensive those tests were;

Results of tests;

Criteria used to determine whether an application or system is deemed Year 2000 ready;

Plans for remediating and retesting any computers, systems or applications that failed Year 2000 tests; and

Individuals responsible for authorizing the testing plan and accepting testing results.

The testing plan should be consistent with the financial institution's Year 2000 contingency plans. The FFIEC intends to issue guidance in the near future on contingency planning for Year 2000.

Testing Internally Developed Systems

Financial institutions with internally developed systems should establish a formal process for testing these systems. The financial institution should test mission-critical systems first. When internal expertise is unavailable, management should retain appropriate external technical expertise to test and to evaluate test results. Financial institutions should follow their established change control processes (under the systems development life cycle [3]) during the remediation and testing process. Financial institutions should conduct testing between the financial institution's internal systems and any interface with external entities.

Testing with Service Providers, Software Vendors, and Other Third Parties

Financial institutions should coordinate and implement (where appropriate) test plans to address the testing with service providers, software vendors and other third parties as discussed in the section on "Testing for Year 2000 Readiness." The following are options for testing with service providers, software vendors, and other third parties.

Service Providers**.** Although it is preferable for financial institutions to test the full range of applications provided by service providers, the results of proxy tests may be acceptable. In proxy testing, the service provider tests with a representative sample of financial institutions who use a particular service on the same platform. Test results then are shared with all similarly situated clients of the service provider. The service provider should make test results available for audit by customers or their representatives. The financial institution is responsible for assessing testing results provided by service providers to determine whether the institution can rely on the proxy test results. The financial institution also should test all systems and interfaces under its direct control.

Software Vendors. Financial institutions should strive to test software provided by software vendors, including turnkey systems, in the financial institution's own environment, to the extent possible. Testing in a financial institution's own environment is preferable because it is the best indicator that their systems are Year 2000 ready. Such testing can be done in a variety of ways, including obtaining a testing package from the software vendor and testing within the financial institution's own test environment. Any interfaces with significant vendor-supplied software also should be tested within the financial institution's own testing environment to confirm that when used together they will function properly.

If the financial institution is unable to test wholly within its own environment, it may test at a contingency or disaster recovery "hot site." The contingency site is a separate facility configured with identical or similar hardware used by the institution to process transactions and produce records if the institution's own environment becomes inoperable. Another option is for a financial institution or a user group to rent or purchase equipment to use for testing. Typically, in these cases, the financial institution must provide the application software and operating system. This testing environment should recreate and test all interfaces and/or exchanges of data between both internal and external systems.

Other Third Parties.Financial institutions should test their mission-critical applications with material third parties to whom they transmit or from whom they receive data. For additional information see "Guidance Concerning The Year

2000 Impact on Customers." Other third parties may include business partners (e.g., credit bureaus), other financial institutions, payment system providers, clearinghouses, customers, and, to the extent possible, utilities.

Testing external interfaces with other financial institutions will verify that each institution's network protocol, business applications, and operating system platforms are performing as expected. Financial institutions should develop various scenarios to verify or test that these interfaces will function as expected. They should consider using point-to point testing and end-to-end testing for transactions such as electronic payments (e.g., ACH, ATM transmittals). Financial institutions should contact their telecommunications and utility companies to discuss the feasibility of testing with them.

VERIFICATION OF TESTING PROCESS

Financial institution management may use internal auditors, external auditors, or other qualified sources to evaluate tests. A verification of the testing process should involve, at a minimum, the project manager, the owner of the system tested, and an objective independent party such as an auditor, consultant, or expert from an independent area. This objective review should critique the Year 2000 tests to ensure that the tests are effective, that key dates are checked, and that changes made resulted in reliable information processing. If the financial institution lacks internal expertise, management should use other qualified professionals, such as management consultants or CPA firms, to provide an independent review. If auditors or consultants are used, they should consult with management during the planning process to ensure that Year 2000 tests can be thoroughly reviewed in a cost-effective manner. If most or all of a financial institution's services are provided by vendors or service providers, management should ensure that the vendors have performed reviews similar to the type described here, and management should receive results of those reviews.

MAINTAINING YEAR 2000 READINESS

In addition to ensuring that existing systems will function properly for critical dates described above, management also should ensure that all new applications, operating systems, software, and hardware are Year 2000 ready before installation. Institutions should test all systems, products and services regardless of when they were upgraded or purchased.

CONCLUSION

The FFIEC expects financial institutions to manage effectively the Year 2000 testing process, regardless of how individual computer systems are developed and operated. The board of directors and management are responsible for ensuring that testing is conducted by the party in the best position to perform the testing. A testing strategy and a written testing plan should be developed for all mission-critical systems and management should review the results of the testing. Management should adhere to the key testing milestone dates outlined in this guidance to help ensure that their financial institutions will be Year 2000 ready.

SOURCES FOR ADDITIONAL INFORMATION

Financial institutions may find additional information on the Year 2000 by researching websites maintained by their software vendors and service providers and others that supply products and services for mission-critical applications. Also, the General Accounting Office's "GAO Year 2000 Guidelines," includes checklists that institutions may find useful. The guidance can be obtained from the GAO or from their website (www.gao.gov). For additional information on the Year 2000 problem, financial institutions also should consult the following helpful websites:

Federal Financial Institutions Examination Council (www.ffiec.gov)
Federal Deposit Insurance Corporation (www.fdic.gov)
Federal Reserve Board (www.frb.gov)
Office of the Comptroller of the Currency (www.occ.treas.gov)
Ofice of Thrift Supervision (www.ots.treas.gov)
National Credit Union Administration (www.ncua.gov)

---

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

2. Although the Gregorian calendar is used throughout most of the world, many computer programs are based on the Julian Calendar.

3. A systems development life cycle is the stages through which software evolves from an idea to implementation.

Interagency Statement

May 13, 1998 statement

GUIDANCE CONCERNING CONTINGENCY PLANNING IN CONNECTION WITH 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) 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 2000readiness 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 problem[1] 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 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.

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[3] event 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;

- 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 servicer 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.

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 .

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/fils/1997/fil9768.html) .

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 .