CEO Memo

RESCINDED

April 3[illegible] 1998

CEO Ltr 82 - FFIEC Guidance Concerning Testing For Year 2000 Readiness

Copy of FFIEC 1998 Y2K Advisory Letter

Any attachments to this document are rescinded only as they relate to national banks and federal savings associations.

Interagency Statement

April 10, 1998 statement

Y2K

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 dates, documentation, and contingency planning.

- Management should ensure that qualified sources verify the testing process.

Key Milestones for Testing Phases

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 implemented 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 res

The testing pla sho consistent with the financial institution's Year 2000 contingency plans. The FFIEC int ds to guidance in the near future on contingency planning for Year 2000.

Testing Internally Dev ped Sy em
Financial institutions with intern y d ped systems should establish a formal process for testing these systems. The fina al in itut should test mission-critical systems first. When internal expertise is unavailable, ma ge ent sh uld retain appropriate external technical expertise to test and to evaluate test re ts. Fin cial institutions should follow their established change control processes (u er the sys s development life cycle [3]) during the remediation and testing process. Financial t tuti s sh ld conduct testing between the financial institution's internal systems and any in fac th external entities.

Testing with Service Providers, Software Vendors, d Ot Third Parties
Financial institutions should coordinate and implement (where pprop ate) test plans to address the testing with service providers, software vendor nd oth third parties as discussed in the section on "Testing for Year 2000 Readiness." The llow are options for testing with service providers, software vendors, and other third parti

- Service Providers. Although it is preferable for financial institut s to t the ull range of applications provided by service providers, the results of pro tests ay be acceptable. In proxy testing, the service provider tests with a repres tative ample of financial institutions who use a particular service on the same platform. 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
- Federal Deposit Insurance Corporation
- Federal Reserve Board
- Office of the Comptroller of the Currency
- Office of Thrift Supervision
- National Credit Union Administration

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.