The Corinthian

Volume 2 Article 5

2000

Year 2000 and the Banking Industry*

Jill Rainey
Georgia College & State University

Year 2000 and the Banking Industry*

Jill Rainey

Faculty Sponsor: Dixie Clark

The Federal Financial Institutions Examination Council (FFIEC) first brought the attention of the banking industry to the Year 2000 problem in 1996 (*Year 2000 Project* 1), but the Year 2000 problem originated many years ago. As a result of limited space, programmers in the 1960s and 1970s began using abbreviations and codes to represent longer words, phrases, and numbers (*FDIC Consumer News—Fall 1998* 2). This shorthand method of indicating dates continued into the computer era and has worked fine until now. On January 1, 2000, things will not be so simple. If the date is recorded in a computer simply as "01-01-00," the "00" could be read by the computer to be "1900," not "2000." That mistake could lead to malfunctions unless computer systems are repaired to process dates correctly in the Year 2000 (*FDIC Consumer News—Fall 1998* 2). The FFIEC and the Federal Deposit Insurance Corporation (FDIC) have monitored and reviewed the preparations of financial institutions for Year 2000. These two agencies have required that institutions meet key milestone dates and complete five phases of preparation: Awareness, Assessment, Renovation, Validation, and Implementation. Financial institutions have met this challenge successfully and are ready to face the Year 2000 with confidence.

The problem with the Year 2000, sometimes referred to as Y2K or the millennium bug, originated with government agencies and large businesses that used "tabulating equipment" before electronic equipment and computers became available in the 1960's and 70's. These machines read, sorted, and tallied information on cards, and if any digit was mistyped, the whole card had to be

redone. With limited space on each card, programmers began using abbreviations and codes to represent longer words, phrases, and numbers. For example, the year 1969 was recorded as "69" with holes keypunched in a card. In turn, the machines were programmed to assume that those two digits signified 1969 (*FDIC Consumer News—Fall 1998* 2).

This shorthand method of recording dates continued into the electronic computer era. The cost and storage problems associated with limited computer memory available before the invention of computer chips motivated the continuation of this shorthand method. Until now, the two-digit arrangement for calendar year has worked fine. When January 1, 2000, comes, however, things will not be so simple. If the date is simply recorded in a computer as "01-01-00," the "00" could be read by the computer to be "1900," not "2000." This mistake could lead to malfunctions unless computer systems are fixed to process the date correctly in the Year 2000 (*FDIC Consumer News—Fall 1998* 2).

"Every business faces risks related to the Year 2000 if its computer system malfunctions or if the companies it does business with have problems with their computers" (*FDIC Consumer News—Fall 1998* 6). Problems can also arise from embedded chips that are in many different types of products ranging from telephones and copy machines to air conditioners and elevators. For banking institutions, concerns include posting interest to deposit accounts, crediting loan payments received, handling automated teller transactions, and much more (*FDIC Consumer News-Fall 1998* 7).

The FDIC and other regulators are working very hard to make sure that financial institutions are prepared for the Year 2000 and are minimizing potential Y2K interruptions. Many government agencies are notifying institutions about what is expected of them regarding this big event. Federal banking regulators have jointly issued guidance to all FDIC-insured institutions on meeting minimum standards for Y2K-related readiness, the most important of which is testing computers. Institutions also have a responsibility to keep customers informed on their banks' Y2K preparation.

FDIC guidance also includes steps for determining whether or not services provided by outside vendors are Year 2000 compliant. Seminars for bankers have been presented all across the country to extend awareness of what federal and state regulators expect. Visits to every FDIC-insured financial institution have been made to monitor the progress of Y2K preparations. These visits have consisted of rigorous examinations to make sure all areas of Year 2000 preparation have been completed. On-site assessments have been done on many of the companies used by the banking industry for computer services and products (*FDIC Consumer News—Fall 1998* 6-7). The FDIC has also given strict key milestone dates (i.e., deadlines) for testing processes to be completed (*Interagency Guidance* FIL-93-98 1).

A five-phase process has been laid out for financial institutions as they discover, plan, and implement their preparations for Year 2000 compliance. The process has five phases: Awareness, Assessment, Renovation, Validation, and Implementation.

In the Awareness Phase, the Year 2000 problem must be defined, and the support of top level management must be gained to gather necessary resources to perform compliance work. A Year 2000 team must be established and an overall strategy developed. This overall strategy or plan should encompass in-house systems, service bureaus for outsourced systems, vendors, auditors, customers, and suppliers. This list should also include all correspondents (FFIEC, *Year 2000 Project* 2).

In the Assessment Phase, an institution must assess the size and complexity of the problem and detail the magnitude of the effort necessary to address Year 2000 issues. All hardware, software, networks, automated teller machines, various processing platforms, and customer and vendor interdependencies possibly affected by the Year 2000 date change should be identified. The highest concern is placed on the financial institution's core processing system. The possibly affected items are termed mission critical. This assessment must also include items dependent on embedded microchips: security systems, elevators, vaults, and telephone systems. Effects of mergers and acquisitions, major system

developments, corporate alliances, and system interdependencies must also be assessed. During this phase, time limits and resource needs should be identified and established. Resources should include skilled personnel, contractors, vendor support, budget allocations, and hardware capacity. Contingency plans should begin to be developed during this time (FFIEC, *Year 2000 Project* 2-3).

Many changes must occur during the third phase, Renovation. Code enhancements, hardware and software upgrades, system replacements, vendor certification, and other associated changes may be necessary. The priorities of work are determined by information discovered in the Assessment Phase. Outside servicers or third-party software providers on which institutions rely will require continuous monitoring to ensure necessary progress (FFIEC, *Year 2000 Project* 3).

The fourth phase, Validation or testing, is the most critical. Although a phase by itself, testing should be done in all phases as any changes are made. Validation includes the testing of incremental changes to hardware and software components as well as connections with other systems. Internal and external users must accept all changes. This acceptance will also require continuous discussion with vendors to determine the success of their validation processes (FFIEC, *Year 2000 Project* 3). For this phase, key milestone dates were established for each financial institution:

- June 30, 1998–Institutions should have completed the development of their written testing strategies and plans. These plans should be made available to supervisory authorities upon request.
- September 1, 1998—Institutional in-house processing departments and service providers should have commenced testing of internal mission-critical systems, including ones 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 depending on service providers for mission-critical systems should be substantially completed. External testing with customers, other financial institutions, business partners, and payment system providers, etc. should have begun.
- June 30, 1999—Testing of mission critical systems should be complete, and implementation should be substantially complete. (FDIC, *Interagency Guidance* FIL-93-98 71-2)

During this stage, precise written documents must be kept to provide an audit trail to aid in the correction of problems if they occur. The documentation should include the type of test performed, an explanation of the choice of tests and their extensiveness, results of the tests, criteria used to determine whether an application or system is considered Year 2000 compliant, 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 (FDIC, *Interagency Guidance* FIL-93-98 7-8).

Implementation is the last stage of preparation. It occurs when all systems are deemed Year 2000 compliant and are fully accepted by all users. For any system not found compliant, the business risk and effect must be determined, and the institution's contingency plan should be put into place. Any non-compliant mission-critical system should be brought to the attention of executive management for immediate resolution. This stage also requires that any new systems or subsequent changes to verified systems be Year 2000 compliant (FFIEC, *Year 2000 Project* 3).

There are many plans and policies required by the FDIC for Year 2000 compliance. Some of these plans should be developed and revised within the phases previously mentioned, and others should be developed in response to a certain need. There must be a Year 2000 Plan, Testing Plan, Contingency Plan, Liquidity Policy, Customer Risk Assessment, and Plan for Customer Awareness and Communication (FFIEC, *Year 200 Work* 2-19).

The Year 2000 Plan should be used as an overall guide for the institution to follow in the process of becoming compliant. It should include a mission statement of what the institution plans to accomplish and a list of inventory needing assessment. This statement should be developed during the Awareness phase of preparation (FFIEC, *Year 2000 Project*).

The Testing Plan is one of the main tools for compliance. A sound plan must be developed and implemented for both internal systems and interfaces with external systems. Institutions serviced by outside providers may rely on proxy testing but are cautioned to assess the provider's reliability. Serious remediation problems could be hidden by a failure to test thoroughly. The failure to identify or correct problems could threaten the safety and soundness of the institution. The plan should include at least the following components: testing environment, testing methodology, testing schedules, human and financial resources, critical test dates, documentation, and contingency planning. The FFIEC expects all key milestones dates mentioned in the Validation Phase to be met. All mission-critical items should be tested first according to their importance to the continuing operations of the institution and the costs and time required to apply a solution. User groups can be formed to evaluate the performance and testing methodologies of service providers and software vendors. These user groups can be very beneficial to financial institutions as a way to exchange ideas and information on testing. There is no certain way to approach testing for the Year 2000. The FFIEC lists the various types of tests that may be done. The testing methodologies are as follows: baseline, unit, integrated, regression, future, user acceptance, point-to-point, and end-to-end. When testing, the financial institution must determine the critical dates that apply to each of the mission-critical items to be tested. The FFIEC recommends that any of the following applicable dates should be tested:

- April 9, 1999—9999 on the Julian calendar. The 99th day of 1999. 9999 denotes the "end of input" in many computer systems.

- September 9, 1999—9999 on the Gregorian calendar. 9999 denotes the "end of input" in many computer programs.
- December 31, 1999—Last day in the 1999 year.
- January 1, 2000—Beginning of the Year 2000.
- January 3, 2000—First business day in the Year 2000.
- January 10, 2000—First day to require a seven 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 the first quarter of 2000.
- October 10, 2000—First date to require an eight-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.

Internal auditors, external auditors, or other qualified sources should verify the testing process (FDIC, *Interagency Guidance* FIL-38-98 1-6).

Also essential for Year 2000 readiness is a Contingency Plan, for which there is no simple or ideal solution. Each financial institution must evaluate its own unique circumstances and environment to develop a comprehensive plan to ensure its ability to continue functioning as a business after January 1, 2000. Senior management and the Board of Directors should attach a high priority to the development, validation, and implementation of the contingency plan (FDIC, *Interagency Guidance* FIL 51-98 2).

There are two types of contingency plans that can be used to alleviate Year 2000 risks. They are the Business Resumption Contingency Plan and the Remediation Contingency Plan (FDIC *Interagency Guidance* FIL-51-98 1). A Business Resumption Contingency Plan includes efforts by financial institutions and their service providers and software vendors to mitigate operational risks if core business processes fail, regardless of whether mission criti-

cal systems were remediated for the Year 2000. This plan is crucial to Year 2000 readiness because an institution must be able to withstand problems that could arise when systems do not operate as expected (FFIEC, *Questions and Answers* 2). The four phases of the Business Resumption Contingency Plan are as follows:

- Organizational Guidelines—Define the business continuity planning strategy.
- Business Impact Analysis—Assess the potential impact of mission-critical systems failure.
- Contingency Plan—Establish a timeline for implementation and action, circumstances, and trigger dates for activation.
- Validation—Design a method so that the business resumption contingency plan can be tested for feasibility. (FDIC, *Interagency Guidance*, FIL-51-98 3)

A Remediation Contingency Plan includes efforts by financial institutions and their service providers and software vendors to alleviate Year 2000 risks associated with the failure to renovate, validate, and implement mission-critical systems to make sure that they are Year 2000 ready (FFIEC, *Questions and Answers* 1). A Remediation Contingency plan is not required if a mission-critical application or system has been remediated, tested, and implemented. If a plan is found to be necessary, at a minimum it should include the following:

- An outline of the alternatives available if remediation efforts are not successful.
- Consideration of the availability of alternative service providers or software vendors.
- Establishment of trigger dates for activating the remediation contingency plan, with account taken of the time necessary to convert to alternate service providers or software vendors. (FDIC, *Interagency Guidance* FIL-51-98 2-3)

A Liquidity Policy is another necessary document for which there is no set structure or form. To satisfy the policy requirements, the financial institution must be able to show that it has a means of obtaining extra cash at the end of the year if necessary. Extra cash will be necessary only if customers panic and decide to withdraw

large amounts of money. According to Brian Smith, for a bank to become significantly more liquid, it has to choose between selling and borrowing. When selling, the bank basically swaps one liquid asset for another. As for borrowing, the most inexpensive source should be used first. With borrowing, long-term assets can be used as collateral to avoid the impact of any rate increase. The Federal Home Loan Bank is offering advances at extremely low rates, and the Federal Reserve Bank has special Y2K offers available through its discount window. Each offer has specific rates, terms, and conditions (38-39). Once the liquidity availability is established, arrangements for cash delivery must be made.

Customer risk is also a major factor in Year 2000 readiness. Many customers (borrowers especially) depend on computer systems that must be Year 2000 compliant. Corporate or business customers who have not considered these issues may experience a disruption in business and suffer potentially significant financial difficulties affecting their ability to repay debts as scheduled (FFIEC, *Year 2000 Project* 4). Processes should be developed to assess customer risk by funds takers, funds providers, and capital market/asset management counter parties. The process should include identifying material customers, evaluating their Year 2000 readiness, assessing their Year 2000 risk to the institution, and implementing appropriate controls to manage and mitigate their Year 2000-related risk to the institution (FFIEC, *Year 2000 Work* 4).

A plan for Customer Awareness and Communication should also be developed. This plan should be designed to respond to questions and to communicate with customers on Year 2000 matters. Effectively responding to customers' inquiries is in the best interests of the financial institution because it will serve to calm the fears and concerns customers may have of Year 2000-related issues. Lowering concern will diminish customer panic and the desire to withdraw large amounts of money from the bank. Each customer is different and will have unique questions. Some may be concerned about the safety of the money in their account, their access to funds after January 1, 2000, or the types of records that

they may need to maintain. The following are ways suggested by the FDIC to present information to customers and to address their concerns:

- 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,
- Develop an Internet site to inform customers of Year 2000 preparation efforts. (FDIC, *Interagency Guidance,* FIL-52-98 2)

The banking industry is one of the most highly regulated industries in the country. Banks are regulated by the FFIEC and the FDIC. Preparation for the century date change started over three years ago and has been going strong since that time. Banks have gone through rigorous examinations to ensure Year 2000 readiness and compliance. Confidence should remain high for customers, employees, and members of the banking industry who know that their institutions are ready. The Year 2000 is a challenge taken with eagerness and excitement by the banking industry, which is fully prepared to step into the next millennium.

**Editors's Note: This article was written in the fall of 1999 when preparations for Y2K were still being made.*

Bibliography

Federal Deposit Insurance Corporation. *FDIC Consumer News–Fall 1998.* Washington, DC: 1998.

— . *Interagency Guidance on Common Questions About FFIEC Year 2000 Policy.* FIL-93-98. Washington, DC: 1998

— . *Interagency Guidance on Testing for Year 2000 Readiness.* FIL-38-98. Washington, DC: 1998.

— . *Interagency Guidance on Contingency Planning for Year 2000 Readiness.* FIL-51-98. Washington, DC: 1998.

— . *Interagency Guidance on Year 2000 Customer Awareness Programs.* FIL-52-98. Washington, DC: 1998.

Federal Financial Institutions Examination Council. *Year 2000 Project Management Awareness.* Interagency Statement. Washington, DC: 1997.

— . *Year 2000 Work Program Phase II.* Version 3.02. Washington, DC: 1999.

— . *Questions and Answers Concerning Year 2000 Contingency Planning.* Washington, DC: 1998.

Smith, Brian. "Y2K and Your Liquidity." *America's Community Banker* October 1999: 38-39. Online. ABI Inform 22 November 1999. <http:www.mariner.galileo.gcsu.edu>.