January 2000

Technology Shifts and the Law: Year 2000 Readiness for Banks and Thrifts

Patricia A. McCoy
Boston College Law School, patricia.mccoy@bc.edu

Follow this and additional works at: https://lawdigitalcommons.bc.edu/lsfp
Part of the Administrative Law Commons, and the Banking and Finance Law Commons

Recommended Citation

This Article is brought to you for free and open access by Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College Law School Faculty Papers by an authorized administrator of Digital Commons @ Boston College Law School. For more information, please contact nick.szydlowski@bc.edu.
I. INTRODUCTION

The advent of new technology is not a static event; rather, it is the beginning of a dynamic process in which old tradeoffs are renegotiated and incompatible standards vie for dominance. Thus, in the railroad industry, the South eventually scrapped narrow-gauge for standard-gauge tracks in the nineteenth century. In the twentieth century, the beta videocassette format was eventually replaced by VHS, computer operating systems evolved toward Windows and blood banks refined their procedures to screen for AIDS.

As this suggests, old generations of technology continually evolve into new generations of technology in order to accommodate change. Sometimes this is to achieve uniformity in standards (as with railroads, VCRs and personal computers) or greater power or speed (as with computer chips). Other times, it is to address risks of imminent harm (as with blood banks and AIDS).

When change is driven by uniform standards or technological improvements, generally the owners of the old technology have the choice of bearing the cost or doing without. But where imminent harm necessitates change, should the law redress potential harm to third parties from a failure to replace the old technology and, if so, how? The law could take a number of stances. First, the law could force owners (or the original manufacturers of the technology) ex ante to install the new technology at their own expense. Second, the law could refrain from intervening ex ante, making replacement a voluntary matter, but require the owners (or the manufacturers) to compensate any harm to third parties ex post. Finally, the law could decline to intervene and let the losses lie where they fall.

The "Year 2000 problem" and the specter of massive computer breakdowns raised these problems with uncommon urgency. As is well
known by now, the Year 2000 problem arose from the inability of hardware and software based on older operating systems to recognize dates after December 31, 1999. In the final analysis, the century date change passed uneventfully and predictions of an apocalyptic breakdown proved unfounded. Pundits later debated whether the enormous efforts to repair the Year 2000 bug were a success or a waste of funds, a question that may never be answered with certainty. The only thing that can be said with any assurance is that the feared damage did not come to pass.

This article chronicles the regime of *ex ante* government regulation that was imposed on the United States banking industry to prevent the Year 2000 problem from materializing. For most industries in the United States, Year 2000 compliance was a voluntary matter and allocation of the risk of harm was left to private contracting and any *ex post* remedies that the legal system might afford. In the financial services industries, however, particularly in securities and banking, there was a different state of affairs. In those industries, the government adopted an intricate system of command-and-control regulation that mandated Year 2000 repairs and compliance through regulatory decrees and examinations, on pain of closure.

Why did financial services undergo a stricter regime of government intervention in comparison with other industries? Ultimately, concerns about financial contagion and systemic risk were the factors that proved decisive. Banks are the glue that binds the payments system and, as such, banks are inextricably linked through electronic funds transfers and correspondent accounts. Due to that interconnectivity, Year 2000 problems at one major bank could have easily spread to others, raising fears about paralysis of the payments system and a halt to general commerce.

The concerns about systemic risk were compounded by the fact that banks were peculiarly vulnerable to breakdowns from the Year 2000 problem. More than in other industries, the overwhelming proportion of what banks did—from interest rate calculations to loan amortization schedules—required date-sensitive calculations. Thus, on average, ninety percent of a bank’s computer operations were “mission critical” in the sense that they were vulnerable to the Year 2000 bug and posed major risk to the institution if any of those operations failed. Furthermore, the computer systems of banks and thrifts were in constant telecommunication with outside computer systems of correspondent banks, automated clearinghouses, etc. That made the banking industry prone to reinfection by outside computer systems if their customers and business partners were not Year

---

1. See Section II infra.
2000 compliant. Compounding matters, smaller institutions were more likely to depend on outside software vendors whose repair efforts were outside of their control.³

The deadline for fixing the Year 2000 problem was uniquely immovable. In a prodigious feat of agency mobilization, federal banking regulators prodded the banking industry — through the bully pulpit, regulations and agency sanctions — to repair the Year 2000 problems in their computer systems. It increasingly became apparent, moreover, that the Year 2000 problem was not just a technological problem. It affected every aspect of a bank’s business, from computer specialists to accountants, from the boardroom to the lowliest teller.

This article surveys the guidelines and guidances that were issued by federal banking regulators on Year 2000 compliance up through the spring of 1999.⁴ The effect of those standards on mergers, acquisitions and other regulatory applications is described.⁵ In addition, the article discusses the SEC’s 1998 interpretive release on the requirements for Year 2000-related disclosures under the federal securities laws.⁶ The article closes with consideration of supervisory actions by federal banking regulators concerning Year 2000 compliance, ranging from agency examinations to enforcement.⁷

II. THE PROBLEM

The Year 2000 problem referred to the inability of computer hardware and software that were based on older operating systems to recognize dates after December 31, 1999. The problem posed systemic safety concerns for the banking industry due to the industry’s heavy reliance on date-sensitive computer calculations.

The Year 2000 problem dated back to the decision by computer programmers in the 1960s to economize on computer memory by coding years between 1900 and 1999 by their last two digits. Thirty to forty years ago, personal computers had not arrived and mainframe computer memory was scarce and prohibitively expensive. Costs could be cut if six bytes of memory were used to designate a date, say by coding April 1, 1968 as 680401 instead of 04/01/1968. Thus, the decision was made to sacrifice the ability to recognize dates before or after the twentieth century for savings in

³ See id. at 399.
⁴ See Section III infra.
⁵ See Section IV.A infra.
⁶ See Section IV.B infra.
⁷ See Section V infra.
memory. As a consequence, software that was imbedded with the old two-digit codes was programmed to assume that dates after December 31, 1999 were dates in the 1900s or even stop functioning altogether.\(^8\)

In the 1960s, with the twenty-first century years off and technological advances occurring at breakneck speed, numerous software designers assumed that operating systems and other software they designed would be discarded long before the millennium arrived, forestalling a Year 2000 problem. Their predictions proved wrong. Later operating systems and software upgrades were grafted onto the original 1960s software, thereby incorporating and perpetuating the old two-digit codes. As the Year 2000 eventually drew near, many businesses were shocked to find that their date-sensitive systems were prone to miscalculation or failure, despite major investments in new software systems.\(^9\)

The Year 2000 problem (also known as Y2K, the century date change or the millennium bug) was of acute concern to banks and bank regulators. Most bank information systems today are highly computerized. By its very nature, moreover, the banking business requires myriad date-sensitive computations. Consider, for example, interest calculations, posting of debits and credits, payment notices, verification of credit card expiration dates, and preauthorized electronic payment orders, not to mention reports to regulators. If Year 2000 problems were not corrected, interest payments could have been calculated as of the early 1900s. Loans could have appeared as a century overdue. Paid-up insurance policies could have been canceled as expired. Amortization schedules could have been miscalculated. Expired credit cards could have been reactivated and valid ATM cards could have been denied authorization. Panicky depositors could have triggered a New


\(^9\) See, e.g., Gerber, supra note 8, at 841, 843–44.
Year’s Eve run on deposits. At worst, vital links in the payment system could have broken down, causing bank payments to grind to a halt.\textsuperscript{10}

There were essentially two solutions to the Year 2000 bug, both of which were straightforward from a programming perspective but costly and time-consuming. One solution was to examine the computer software for every depository institution to detect and correct the two-digit date codes. That necessitated hiring programmers (often trained in Fortran and COBOL in the 1960s and 1970s) at a cost of $1 or more per line, to sift through billions of lines of code. The other solution was to throw out a bank’s old software entirely and install a whole new system, often with new hardware, that was Year-2000 compliant.\textsuperscript{11} In some cases, lack of funds necessitated short-term repairs, followed by outright replacement after January 1, 2000.\textsuperscript{12}

Either way, the solution was staggeringly expensive and the cost kept rising with time. As January 1, 2000 approached, trained programmers were in ever-increasing demand and their fees continued to mount. Total outlays by the banking industry for Year 2000 readiness were expected to exceed $10 billion and may have topped half a billion dollars apiece for the largest U.S. banks.\textsuperscript{13}

The overwhelming proportion of banks and thrifts fixed their internal Year 2000 problems.\textsuperscript{14} However, the problem was not self-contained. Repairing the bank’s software was not enough. By necessity, virtually every depository institution exchanged data over computer lines with other institutions, customers and regulators. Any incoming data from the outside that was infected with the Year 2000 problem could reinfect the computer system of the bank. Banks could lose revenue due to reduced deposits and loan defaults if unprepared corporate customers suffered business


\textsuperscript{11} See, e.g., Keehan & Peterson, supra note 8, at 482–83.

\textsuperscript{12} See FFIEC, Year 2000 Project Management Awareness (visited May 5, 1997) <http://www.ffiec.gov/y2k/advisory2.htm> [hereinafter Project Management Awareness].

\textsuperscript{13} See, e.g., R. Christian Bruce, OCC Cuts a CD for National Banks To Help Assess Year 2000 Preparations, 71 BNA BANKING REP. 908, 909 (1998); Eileen Canning, Year 2000: Bankers Will Spend More Than Expected on Y2K Compliance Efforts, Officials Say, 71 BNA BANKING REP. 827 (1998); Greaves, supra note 2, at 390.

\textsuperscript{14} The accounting firm Grant Thornton LLP reported, for example, that 98 percent of 815 community banks surveyed were confident that their repairs would be in place when 2000 arrived. See Community Banks Sure About Y2K Readiness; Less Confident About Customers, Study Says, 72 BNA BANKING REP. 331 (1999).
interruptions or failures due to Year 2000 computer problems of their own. Extra cash had to be on hand to meet demand for funds by worried depositors. Finally, banks faced service interruptions if the operations of their outside vendors shut down due to internal Year 2000 problems. These problems were compounded when dealing with businesses located abroad, where Year 2000 readiness was even further behind. Because banks had to rely on the Year 2000 readiness of outside firms, the preparedness of the business community at large was the weak link in the chain and one that was not fully within banks' control.15

III. FEDERAL STANDARDS FOR FIXING THE YEAR 2000 PROBLEM

Beginning in 1997, federal banking regulators issued a series of guidances and guidelines designed to ensure that banks and thrifts attained Year 2000 readiness. The Year 2000 remediation process was divided into six stages, consisting of awareness, assessment, repairs, testing, implementation and contingency planning.

Determined to avoid a meltdown of the nation’s banking system, federal banking regulators, along with the Federal Financial Institutions Examination Council (FFIEC), prodded banks and thrifts since 1996 to become Year 2000 compliant. Pressure from federal regulators stepped up after it became apparent in 1997 that large segments of the banking system were oblivious to the impending Year 2000 glitch. Two years later, there was a remarkable turnaround and the banking industry was among the most prepared of all American industries. The Year 2000 compliance efforts of federal banking regulators were a remarkable story of agency mobilization and resolve in the face of an immovable and potentially catastrophic deadline.

FFIEC first issued a call for action on the century date change in an interagency statement titled "The Effect of Year 2000 on Computer Systems" in June 1996. Initially, federal regulators issued safety and soundness standards for Year 2000 compliance in the form of a series of guidance papers published under the auspices of FFIEC.16 The first eight

15 See id.
guidances culminated in the issuance of interim joint interagency guidelines on Year 2000 standards for safety and soundness of banks and thrifts, which were published on October 15, 1998 and took effect immediately. The agencies invited comment on the guidelines for a sixty day period.

The guidelines, which will be referred to throughout as the "Year 2000 Guidelines" or "the Guidelines," were intended to supplement, not supplant, FFIEC's guidances, which continued to apply to insured institutions and their affiliates. The Year 2000 Guidelines described essential steps that insured banks and thrifts were required to take to assure Year 2000 readiness. While the standards were couched as guidelines, they were mandatory in effect. By law, the Guidelines only applied to insured depository institutions, not to bank holding companies or U.S. offices of foreign banking organizations. Nonetheless, regulators expected regulated entities other than insured banks and thrifts to comply with the FFIEC guidances, under pain of federal sanctions.

---


18 See Interagency Guidelines, supra note 17, at 55,480–81.

19 See id. at 55,481.

20 See id. at 55,482; see generally 12 U.S.C. § 1818.
Authority for the Year 2000 Guidelines came from 12 U.S.C. § 1831p-1, which requires federal banking regulators to establish operational and managerial standards for insured banks and thrifts on internal controls, information systems and internal audit systems.\(^{21}\) Standards under Section 1831p-1 may either take the form of regulations or guidelines.\(^{22}\) For the topic of Year 2000 readiness, federal regulators decided to proceed by way of guidelines to preserve their flexibility to take appropriate supervisory action against institutions that failed to comply.\(^{23}\) On the same date that the Year 2000 Guidelines were published, regulators also amended the regulations implementing the safety and soundness provisions in Section 1831p-1 in order to incorporate the Guidelines.\(^{24}\) The Year 2000 Guidelines divided the Year 2000 remediation process into six phases, consisting of awareness, assessment, renovation, testing, contingency planning and implementation.

A. Awareness And Assessment

Awareness and assessment of the problem were the first steps on the road to Year 2000 readiness. Since 1996, federal banking regulators were increasingly insistent that leadership and support for Year 2000 compliance came directly from the executive suite and the boardroom. Thus, it was incumbent on management and the board to assemble a Year 2000 management team that was led by a senior manager, to provide that team with sufficient funds and personnel, and to set an example by emphasizing Year 2000 compliance as a high priority of the institution.\(^{25}\) A budget had to be established with sufficient funds to pay for personnel with appropriate skills, contractors, vendor support, software development and new hardware (keeping in mind that obtaining and retaining qualified staff became increasingly harder as the Year 2000 deadline approached). Regulators stressed the importance of corporate accountability by requiring direct reporting to top management and the board and clear lines of command and responsibility.\(^{26}\)

In the assessment phase, the size and complexity of the Year 2000 problem had to be assessed and solutions identified. It was not cost-

\(^{21}\) See generally Joseph Jude Norton & Sherry Castle Whitley, BANKING LAW MANUAL § 13.02 (Patricia A. McCoy ed., Dec. 1998).


\(^{23}\) See Interagency Guidelines, supra note 17, at 55,481–82. See Section V.B infra for a discussion of agency enforcement.

\(^{24}\) See Interagency Guidelines, supra note 17, at 55,486.

\(^{25}\) See, e.g., Year 2000 Business Risk, supra note 16; Project Management Awareness, supra note 12; Computer Systems, supra note 16.

\(^{26}\) See Project Management Awareness, supra note 12.
effective, let alone possible, to revise or replace every line of infected code. Recognizing that fact, federal banking regulators required banks and thrifts to come up with an action plan and employ a triage system to identify which systems, applications and software were crucial to their business. This basic requirement was embodied in the command that every bank and thrift had to inventory their hardware and software systems, identify all internal and external "mission-critical systems" that were not Year 2000 ready and prepare a project plan to achieve Year 2000 compliance. Institutions also had to make plans for fixing lower priority systems sometime later after critical repairs were completed. The awareness and assessment phases were to have been completed by September 30, 1997.

Three terms were key to understanding the priorities for triage. The first was the term "mission-critical systems." Mission-critical systems were defined as applications, systems and software that were vital to the successful continuance of a core business activity. Applications, systems and software could also be mission-critical if they interfaced with a mission-critical system.

The second key term was "internal system." An internal system was any digital system whose repair the bank or thrift controlled. Internal systems included software, operating systems, mainframe computers, personal computers, ATM machines, readers/sorters and proof machines, as well as environmental systems that depended on embedded microchips (such as heating and cooling systems, vaults, communications, security systems and elevators).

During the assessment phase, institutions were required to set priorities for repairing internal systems that were mission-critical and paying for those repairs (which the agencies referred to as "renovation"). The initial task of the institution's Year 2000 team was to identify systems qualifying for triage (including systems in remote or overseas offices) and decide whether those systems should be modified, replaced, outsourced or discontinued. Once those decisions were made, the team had to establish reasonable deadlines for commencing and completing repairs or replacement.

See Interagency Guidelines, supra note 17, at 55,484.
See Project Management Awareness, supra note 12.
See Institution Due Diligence, supra note 16.
See Interagency Guidelines, supra note 17, at 55,484.
See id.; Project Management Awareness, supra note 12.
See Interagency Guidelines, supra note 17, at 55,484; Computer Systems, supra note 16. Year 2000 plans also needed to address the so-called "leap year" issue, i.e., the ability of computers to recognize the date February 29, 2000. See Project Management Awareness, supra note 12.
Finally, "external systems" that were mission-critical had to be scrutinized for needed repairs. An external system was one whose repair was not within the control of the affected bank or thrift. External systems included systems furnished by outside data processing service providers or software vendors. In addition, external systems included electronic data exchange systems with other institutions such as correspondent banks, their customers and regulators.\(^{33}\) For data exchanges, it was important to identify what types of electronic data exchanges were operating and how those data exchanges differed from one another.\(^{34}\) Special risks were posed where institutions did business on an electronic basis globally with foreign institutions that were not Year 2000 ready.\(^{35}\)

For software vendors and other third party suppliers, banks and thrifts had to establish a due diligence process to monitor and evaluate their efforts to achieve Year 2000 readiness.\(^{36}\) Management was required to evaluate vendors' own readiness plans and actively monitor project milestones. It was crucial that management obtain assurance that vendors had the funds and personnel to complete their own Year 2000 compliance so that they could honor their contractual obligations to provide uninterrupted service. It was similarly crucial that vendors certify Year 2000 compliance for all work or services that they performed. Federal regulators required management to review vendor contracts to determine who would bear the costs of Year 2000 compliance and to renegotiate those contracts where necessary to include Year 2000 covenants. Where a vendor refused to agree to such a covenant, the institution was required to weigh the cost of terminating the contract and replacing the service or product. The institution had to terminate the relationship with the vendor where the safety and soundness of the institution was at risk.\(^{37}\)

Whenever institutions made new purchases of systems, software or hardware, they had to require the seller to certify in writing that the purchase

---

\(^{33}\) See Interagency Guidelines Establishing Year 2000 Standards for Safety and Soundness, 63 Fed. Reg. at 55,484. External systems reviewed had to include payment system providers such as wire transfer systems, automated clearing houses, check clearing providers, credit card merchant and issuing systems, ATM networks, electronic data interchange systems and electronic benefits transfer systems. See Project Management Awareness, supra note 12.

\(^{34}\) See Project Management Awareness, supra note 12.


\(^{36}\) Interagency Guidelines, supra note 17, at 55,484.

\(^{37}\) See Institution Due Diligence, supra note 16.
was Year 2000 compliant. Such sales contracts were required to include language along the following lines: A “[Licensor] [Seller] represents and warrants that the software will not fail or produce anomalous or incorrect results with respect to data, calculations, and other processing involving dates after December 31, 1999.” Where sellers resisted such clauses, institutions could use statements in the FFIEC guidances that required banks to modify or terminate vendor contracts as negotiating leverage where vendors sought to limit their total liability and exclude damages for lost profits and other forms of consequential damages.

Similar considerations applied to hiring personnel to make Year 2000 repairs or system overhauls. Those personnel had to be under contract whenever possible to ensure that they would be available when needed. They had to guarantee that their work would be Year 2000 compliant.

Once management had identified the mission-critical products and services supplied by service providers and software vendors, it was required to request the following information from those suppliers:

- Information on the vendors’ Year 2000 project plans, including the scope of such efforts, a summary of resource commitments, target dates for repairs and testing and anticipated dates of delivery for Year 2000 products and services;
- Any plans to discontinue or extensively modify existing services and products;
- Regular updates on suppliers’ progress in meeting their own Year 2000 timetables;
- Estimates of the product and support costs to the institution for repairs and testing; and
- The suppliers’ contingency plans in case they failed to successfully complete their Year 2000 plans.

In repairing external software or systems, institutions needed to be aware that adverse legal consequences could flow from unilaterally rewriting computer code. Service providers and software vendors typically included clauses in their original service contracts to the effect that unauthorized code modifications would render warranties and service contracts null and void. Similarly, many software licenses forbade users from providing third parties with access to the software without the licensor’s consent as illegal copyright

---

38 See Project Management Awareness, supra note 12.
39 Keehan & Peterson, supra note 8, at 484.
40 See id.
41 See Project Management Awareness, supra note 16.
42 See Institution Due Diligence, supra note 16.
infringement. Confronted with such clauses, institutions had to make a difficult choice between avoiding the risk of suit and the urgency of attaining Year 2000 readiness.

The assessment phase was to culminate in a Year 2000 project plan that mapped out timetables and plans for each phase of repair work, testing, implementation and contingency planning. Plans were required to address:

- The tasks to be accomplished throughout the duration of the project;
- The necessary resources and the individuals who were responsible for each phase of the project;
- Specific dates for completing key elements of the project; and
- Strategies for responding to inquiries from customers and business partners regarding Year 2000 readiness.

Institutions that had comparable plans in place when the Guidelines were adopted were not required to draft new plans, assuming that their existing plans met with agency approval.

B. Customer Risk

Part of the external Year 2000 threat to depository institutions arose from liquidity concerns if customers such as fund providers, fund takers or capital market or asset management counter parties such as derivatives customers defaulted on their contractual obligations due to their own Year 2000 problems. Depositors and other fund providers potentially posed liquidity risks if they were unable to provide funds or fulfill their funding commitments to institutions. Funds takers such as borrowers and bond issuers who borrowed or used bank funds potentially posed credit risk through defaults on loan or bond payments. Finally, an institution’s market trading, treasury operations and fiduciary activities could have suffered if customers who were active in domestic and global financial markets were unable to settle transactions due to operations problems arising from the Year 2000 date change.

To reduce that exposure, the Year 2000 Guidelines required senior management of banks and thrifts to develop and implement written due diligence procedures to identify customers who posed material Year 2000-

---

43 See Greaves, supra note 2, at 423.
44 See Institution Due Diligence supra note 1; Greaves, supra note 2, at 423–24.
45 See Year 2000 Business Risk, supra note 16.
46 See Interagency Guidelines, supra note 17, at 55,481; Project Management Awareness, supra note 12.
47 See Year 2000 Impact on Customers, supra note 16.
related risks to the institution. By June 30, 1998, institutions were required to implement their due diligence processes. Assessments of individual customers' Year 2000 preparedness and the resulting impact on each bank or thrift were to have been completed by September 30, 1998.

Based on those assessments, management was expected to implement appropriate risk controls (including controls for underwriting risk) to manage and mitigate the Year 2000 risk posed by the institution's customers.\textsuperscript{48} Those risk controls could be tailored to the institution's size, culture, appetite for risk, the complexity of customers' information and operating systems, and the institution's overall Year 2000 exposure. In smaller community institutions, customers might not have been as dependent on information technology as clients of larger institutions and thus the due diligence processes in those institutions did not need to be as extensive or formal.\textsuperscript{49}

In a FFIEC guidance dated March 17, 1998 titled "Guidance Concerning the Year 2000 Impact on Customers," federal regulators outlined their expectations for due diligence as to customer risk. According to the guidance, due diligence was to accomplish the following objectives:

1. \textit{Identify Material Customers Posing Year 2000 Risk}: Management had to identify customers, including customers abroad, that posed material risk to the institution due to lack of preparedness for the century date change. Material risk exposure could depend on the following factors, where applicable:
   - The size of the overall relationship with the customer;
   - The risk rating of borrowers and other funds takers;
   - The complexity of the customer's operating and information technology systems;
   - The customer's reliance on technology for successful business operations;
   - The collateral exposure of borrowers;
   - The funding volume or credit sensitivity of funds providers;
   - The degree of management oversight of Year 2000 repairs by the customer;
   - The resources the customer had committed to its Year 2000 projects; and


\textsuperscript{49} See Year 2000 Impact on Customers, supra note 16.
• The customer's dependence on third party providers of data processing services or products.

(2) **Assess The Year 2000 Readiness Of Material Customers:** Each customer who was identified as material had to be assessed for its Year 2000 preparedness. Management was required to train account officers to perform a basic assessment of the Year 2000 risk posed by customers. To that end, the institution was required to develop one or more standardized questionnaires for eliciting customer response.\(^{50}\)

For customers who either used manual systems or depended on commercial software products and services, this assessment could be less involved and did not necessarily require additional risk management oversight. Customers' Year 2000 readiness was to be reevaluated at least semiannually, and quarterly for customers who posed significant Year 2000 risk. The results of the Year 2000 assessments, ensuing discussions and status updates were to be documented in customers' individual files.

(3) **Evaluate Year 2000 Risk To The Institution:** After identifying and surveying material customers, management was required to assess the Year 2000 risk that those customers posed to the institution, both individually and collectively. Management had to determine whether risk exposure was high, medium or low.

(4) **Develop Appropriate Risk Controls:** Once the level of customer risk was determined, management had to develop and institute appropriate controls to control that risk. Senior management needed to be actively engaged in developing those controls and assuring their timely implementation. Frequently, the types of risk controls that had to be instituted depended on the category of customer. Federal regulators prescribed the following special risk controls for funds takers, funds providers and capital market and asset management counterparties: \(^{51}\)

(a) **Borrowers And Bond Issuers ("Funds Takers"):** During the credit underwriting process, management

\(^{50}\) Appendices A–D of *Year 2000 Impact on Customers*, supra note 16, contained sample questionnaires that some depository institutions used to assess customer readiness.

\(^{51}\) See *Year 2000 Impact on Customers*, supra note 16.
had to evaluate the extent of the borrower’s Year 2000 risk. Underwriters needed sufficient training to enable them to conduct a basic assessment of the applicant’s Year 2000 risk. They had to then evaluate whether that risk would materially affect the applicant’s cash flow, balance sheet or the value of the supporting collateral. Once credit was approved, the loan documentation had to include language that would permit the institution to monitor and manage the customer’s Year 2000 risk. Institutions had to consider incorporating the following clauses into their loan agreements and supporting documentation:

- Borrower representations that Year 2000 programs were in place;
- Representations that borrowers would disclose Year 2000 plans to the lender, provide periodic updates on their progress under those plans and provide copies of any third-party assessments of the borrower’s Year 2000 readiness;
- Clauses requiring audits on Year 2000 issues;
- Covenants ensuring that adequate resources would be committed to completing the Year 2000 plan on time; and
- Default provisions allowing the lender to accelerate the maturity of the debt for noncompliance with Year 2000 covenants.

After the loan or bond offering closed, the institution needed to conduct progress reports on customer Year 2000 preparedness as part of its ongoing credit

---

Senior management of banks and thrifts were expected to establish procedures to identify, assess and control potential Year 2000 risk in their lending and investment portfolios. For example, when performing follow-up credit analyses, loan officers had to determine whether the customer’s Year 2000 risk required an adjustment to its internal risk rating. Similarly, periodic reviews of the adequacy of loan and lease loss provisions had to take account of customers’ Year 2000 risk. If a customer’s creditworthiness deteriorated due to Year 2000 problems, loan and lease loss provisions had to be increased sufficiently to reflect the increased credit risk. Where necessary, loans had to be classified or written off. Management’s analysis of the inherent loss in loan and bond portfolios overall also had to reflect Year 2000 risk posed by customers. (b) Depositors And Other Funds Providers: As with borrowers, management had to identify significant depositors and other funds providers, evaluate their Year 2000 readiness where possible and assess the associated Year 2000 risks. Management needed to be cognizant of concentrations (including concentrations in any single currency) from an individual provider or group of providers who might not have been Year 2000 ready. This risk assessment had to be incorporated into the institution’s contingency plan for liquidity. The contingency plan was required to evaluate a number of scenarios based on different assumptions about the timing or magnitude of funds shortfalls due to Year 2000-related problems. Where an institution had significant funds flows in different currencies, it needed a separate contingency plan for each major

53 See also Project Management Awareness, supra note 12.
54 See Year 2000 Business Risk, supra note 16.
55 For a good general overview of the Year 2000 issues presented by borrowers, see Jay Golter & Paloma Hawry, What Every Loan Officer Needs to Know about the Year 2000 Computer Problem (But Doesn’t Know How to Ask), 10 FDIC BANKING REV. 1 (1997).
currency. The ability to plan for and mitigate potential liquidity risks was aided by the fact that the trigger date for those risks was already known. For instance, institutions were advised to extend the maturity of their advances under funding lines sufficiently past January 1, 2000 to provide time to assess the effect of Year 2000 on their funds providers. Maintaining close contact with funding sources throughout the critical New Year’s Day 2000 weekend also provided management with timely, market-sensitive information essential to effective liquidity planning.

(c) Capital Market And Asset Management Counter Parties: Year 2000 concerns with securities or derivatives customers ranged from the customer’s failure to complete a transaction, with potential to lead to a systemic liquidity crisis, to the customer’s financial failure, possibly leading to total loss of the value of the payment or contract. Furthermore, where an institution was acting in a fiduciary capacity, a counter party’s failure to remit bond payments, fund employer pension contributions or settle securities transactions could heighten the institution’s fiduciary risk. An institution’s first task in this regard was to identify customers who posed large exposures to the bank and/or fiduciary account beneficiaries. The Year 2000 readiness of those customers had to be appraised. Where the institution did not have sufficient assurance that those customers would achieve readiness on time, management was to pursue mitigation measures such as early termination agreements, additional collateral, netting arrangements and third-party

56 See Christian A. Johnson, Year 2000 Credit Risk and Derivatives: Insulating Banks From Counterparty Meltdown, 9 BANKING L.J. 930 (1998) for a discussion of additional actions banks and thrifts could have taken to address the risk of counterparty defaults due to Year 2000 malfunctions.

57 See also Fiduciary Services, supra note 16.
payment arrangement or guarantees.\(^{58}\) Where a
customer posed high uncertainty, the bank or thrift
had to consider avoiding any transactions with that
The interest rate effect of material mismatches of
funding, or maturity, also had to be assessed as
maturity and settlement risk were adjusted. The
institution was not to resume normal transaction
activities with the customer until it demonstrated
that it would in fact be prepared for the century date
change.

\(\text{(d)}\)

**Special Considerations For Institutions Acting As
Fiduciaries:** In addition to the normal due diligence
just described for capital market and asset
management counter parties, institutions that offered
fiduciary services needed to evaluate the potential
Year 2000 risks from managing client assets.
Account assets had to be thoroughly reviewed to
ascertain potential liability or exposure attributable
to issuers of securities with Year 2000 problems.
Certain types of assets, such as closely held
companies, partnership interests, and income
producing real estate, could also have been the
source of possible Year 2000 exposure. If an
institution relied on third party service providers
such as transfer agents, depositories, investment
advisors, custodial agencies and the like to meet
their fiduciary duties, the institution had to evaluate
the Year 2000 readiness of those providers and
make contingency plans in case their services went
awry. In consultation with counsel, disclosures to
beneficiaries about the institution’s Year 2000
preparations and significant Year 2000 issues with
third parties, counter parties and specific asset
holding in customer accounts were advised to reduce
the risk of litigation.\(^{59}\)

\(^{58}\) Christian Johnson urged banks to have the Master Agreement developed by the
International Swaps and Derivatives Association (ISDA) in place prior to doing any

\(^{59}\) See *Fiduciary Services*, *supra* note 16.
From a business standpoint, the due diligence that was required of customers was undoubtedly one of the most sensitive aspects of Year 2000 readiness. The due diligence requirements listed above could endanger longstanding relationships with valued customers. Customers might have been unwilling to produce volumes of confidential information, particularly when their agreements did not have covenants that required them to cooperate. Where documentation did not require access, occasionally there was little more the institution could do than refuse to do business in the future if the customer did not comply. Rather than cooperate, however, some customers may have shifted their business to non-bank financial service providers who did not make intrusive demands for information. Banks and thrifts thus were forced to weigh whether potential defection by customers was worth the business and legal risk of lack of Year 2000 readiness, mindful that a customer's non-cooperation could have been a harbinger of serious problems.

To some extent, banks could avoid having tensions reach the boiling point by working in advance to forestall any problem. In the lending area, for example, if a bank had concern that a borrower's progress toward Year 2000 preparedness was so slow that the bank eventually might have to write down the loan, the bank was advised to contact the borrower as far as possible in advance to give it an opportunity to fix the problem. Banks also preserved their flexibility in dealing with borrowers by satisfying examiners that they had an effective due diligence process in place for monitoring the Year 2000 progress of creditors.60

C. Repairs And / Or Replacement ("Renovation")

The Year 2000 Guidelines used the term "renovation" to refer to the process of repair and replacement. Renovation included code enhancements, hardware and software upgrades, system replacements, and other related changes that ensured that an institution's mission-critical systems and applications were Year 2000 ready.61 Federal regulators vigorously discouraged institutions from using operating systems or other components that were not Year 2000 ready because unanticipated problems could arise.62 Under the Year 2000 Guidelines, repairs of internal mission-critical systems had to be completed in time to substantially complete testing of those repairs by December 31, 1998.63

60 See Keehan & Peterson, supra note 8, at 484.
61 See Interagency Guidelines, supra note 17, at 55,484.
62 See Questions and Answers, supra note 8.
63 See Interagency Guidelines, supra note 17 at 55,484.
The deadline for completing repairs of external mission-critical systems fell three months later. Under the Guidelines, banks and thrifts were required to determine the ability of third party suppliers to make needed repairs to external mission-critical systems in time to substantially complete testing of those repairs by March 31, 1999. In addition, institutions had to develop a written, ongoing due diligence process to monitor and evaluate the efforts of third party suppliers to achieve Year 2000 readiness. As part of that process, banks and thrifts had to keep written documentation of their communications with outside suppliers as to their ability to make timely and effective repairs. Repair efforts of third party suppliers had to be monitored at least quarterly.

In addition, institutions were required to review their contracts with outside suppliers to determine the parties' rights and obligations to achieve Year 2000 compliance. Some outside service providers and software vendors were unable or unwilling to correct Year 2000 problems. In some cases, the developers of software or hardware had gone out of business or no longer supported the application or system in question. Source code was not always available or equipment sometimes had components that were no longer manufactured. Major software providers were sometimes unwilling to provide specific reconfiguration instructions that were tailored to the institution's individual system. To address these problems, federal regulators broadened their Year 2000 examinations to include service providers and software vendors and announced that they would share results from those examinations with affected banks and thrifts. (Federal regulators stressed, however, that they would not certify service providers as Year 2000 compliant). Federal regulators also exerted pressure on those providers to provide the fullest information possible to their customers.

D. Testing

Testing of repairs was just as important as the repairs themselves. Federal regulators described testing as "the most critical phase of the Year

---

64 See id. at 55,484–85; Institution Due Diligence, supra note 16.
65 See Questions and Answers, supra note 8; Institution Due Diligence, supra note 16. FFIEC established a Year 2000 examination program for at least sixteen large service providers and a sister program for at least twenty two large software vendors. Those providers and vendors furnished data processing for, or provided software to, a large number of financial institutions regulated by more than one agency. Each of those suppliers potentially posed a high degree of systemic risk. FFIEC disclosed examination results for service providers to client institutions as a matter of course. It disclosed examination results for software vendors to client institutions only with the vendor's consent.
66 See Institution Due Diligence, supra note 16.
2000 readiness process" and one that could easily consume fifty to sixty percent of the time, funding and personnel dedicated to an institution's Year 2000 project.\(^6\) Regulators warned that failure to perform adequate testing "pose[d] a risk to the safe and sound operation" of an institution and could "mask serious remediation problems."\(^6\)

Testing was complicated by the fact that the software and hardware changes that were needed for Year 2000 compliance could have affected many or all of an institution's internal systems, as well as interfaces with internal and external suppliers, customers and business partners. Accordingly, testing needs varied according to the institution. Mission-critical systems were to be tested first, due to their importance to an institution's operations and the urgency of finding an alternate solution if testing failed.\(^6\) Testing had to be designed so as not to interfere with day-to-day processing activities. All tests had to be conducted by whomever was in the best position to perform tests and assess the results.\(^7\)

The Year 2000 Guidelines set staged deadlines for testing mission-critical systems. Substantially complete testing of internal mission-critical systems was to have been completed by December 31, 1998. Testing of external mission-critical systems was to commence by January 1, 1999 and to be substantially completed three months later, on March 31.\(^7\) Testing with third parties (other than suppliers) with whom the bank or thrift exchanged electronic data (known as "other material third parties" and including credit bureaus and other business partners, other banks and thrifts, payment system providers, clearinghouses, customers and utilities) had to begin by March 31, 1999.\(^7\) June 30, 1999 was the final deadline for testing all mission-critical systems.\(^7\)

The testing process started with developing and implementing effective written plans for testing both internal and external systems. Federal regulators expected those plans to address the testing environment, testing methodology, testing schedules, budget projections, the identity of

\(^{67}\) See Testing for Year 2000 Readiness, supra note 16; see also Interagency Guidelines, supra note 17, at 55,482.

\(^{68}\) Interagency Guidelines, supra note 17, at 55,482.

\(^{69}\) See Testing for Year 2000 Readiness, supra note 16.

\(^{70}\) See Interagency Guidelines, supra note 17, at 55,485; Testing for Year 2000 Readiness, supra note 16; Project Management Awareness, supra note 12.

\(^{71}\) See Interagency Guidelines, supra note 17, at 55,485; Testing for Year 2000 Readiness, supra note 16.

\(^{72}\) See Interagency Guidelines, supra note 17, at 55,484–85; Testing for Year 2000 Readiness, supra note 16; see also Questions and Answers, supra note 8.

\(^{73}\) See Interagency Guidelines, supra note 17, at 55,485; Testing for Year 2000 Readiness, supra note 16.
Testing plans were to contain the following elements:\footnote{74}{See Interagency Guidelines, supra note 17, at 55,485; Testing for Year 2000 Readiness, supra note 16; Project Management Awareness, supra note 12.} \footnote{75}{See Testing for Year 2000 Readiness, supra note 16.} \footnote{76}{See Testing for Year 2000 Readiness, supra note 16, for a discussion of test methodologies.} \footnote{77}{See Questions and Answers, supra note 8. When service providers conducted proxy tests, those tests were to be conducted on institutions of the same type and complexity and use identical versions of the software, operating systems and hardware. Client institutions were required to define the scope and objectives of such tests. Test results had to be documented, validated and assessed to determine their reliability. Institutions were required to independently test any functions of their systems that were not covered by proxy tests. Federal regulators also allowed proxy testing of turnkey software packages provided by software vendors on the same conditions. See id. Proxy tests were not appropriate where the institution modified the software code. In addition, where proxy tests were properly used, institutions had to test internal and external interfaces not covered by the tests and other items under their control. See id.} \footnote{78}{See Questions and Answers, supra note 8.} \footnote{79}{See id.}

- **Testing Environment**: This element considered whether to use current operating computers or a separate computer system to test.

- **Test Methodology**: This segment identified the types of tests that were needed.\footnote{76}{Although regulators preferred that systems be tested in an institution's own environment, that was not always possible for institutions that relied on service providers or software purchased from vendors. In such cases, banks or thrifts were allowed to rely on proxy tests—tests performed on a representative sample of financial institutions that used the same service on the same platform—conducted by service providers or user groups, so long as those tests were appropriate. Alternatively, institutions could have tested their upgraded applications at hot-site locations (disaster recovery sites) so long as tests were run on the same hardware and operating systems. Banks and thrifts were strongly advised not to test system clocks by rolling dates forward without consulting with the manufacturer or vendor. Similarly, reliance on proxy tests were not appropriate where the institution modified the software code. In addition, where proxy tests were properly used, institutions had to test internal and external interfaces not covered by the tests and other items under their control. See id.}
certification by a nationally recognized organization was not a substitute for actual tests.\(^{80}\)

- **Test Schedule:** Timetables had to be established for testing software, hardware and interfaces between systems. Test schedules needed to be coordinated with the test schedules of third parties.

- **Personnel And Funds:** A testing budget had to be established and testing personnel identified.

- **Critical Test Dates:** January 1, 2000 was not the only date with the potential for confusion. Other dates, such as 9999 on the Julian and Gregorian calendars (respectively April 9 and September 9, 1999), and leap year day (February 29, 2000) could wreak havoc if the Year 2000 bug was not fixed.\(^{81}\) Institutions were required to determine what dates their systems were prone to misread and test to make certain that their applications and systems would operate properly when confronted with those dates.

- **Documentation:** Each stage of the testing process had to be documented to make it easier to pinpoint the source of any problems if testing failed. Documentation had to be sufficient to enable a reasonably knowledgeable person to understand which tests were performed on which applications, systems or hardware, what the results were, and how those results were validated.\(^{82}\) This documentation had

---

\(^{80}\) See id.

\(^{81}\) See Testing for Year 2000 Readiness, supra note 16, for a list of possibly troublesome dates. Institutions did not need to test listed dates if those dates were not critical to particular applications. Conversely, institutions had to test other dates that did not appear on the FFIEC list but that could prove troublesome. See Questions and Answers, supra note 8.

\(^{82}\) Regulators advised retaining, among other things, documentation of the following: the institution's overall Year 2000 plan and Year 2000 testing plan; the types of tests performed (e.g., baseline, unit, regression) and a summary of the results; the reason why the institution chose the tests and the extensiveness of the tests; the criteria used to determine whether an application or system was Year 2000 ready; plans for repairing and re-testing any computers, systems or application that failed the tests; names of the individuals responsible for authorizing the testing plan and accepting test results; communications with service providers and software vendors, including any assurances regarding their services or products; copies of any in-house programs that produced test results; and any other documentation that the institution believed supported its decisions, conclusions and due diligence. See Questions and Answers, supra note 8.
to be retained both for purposes of examinations and to enable the institution to demonstrate that it fulfilled its responsibilities in the event of litigation.\(^8\)

Where the system being tested was an external system that interfaced with an outside computer system or was under third-party control, it was crucial to coordinate inside tests with outside testing.\(^8\) If outside service providers or software vendors conducted the testing, federal regulators expected senior management to monitor the process and obtain satisfactory assurances that the systems were properly and successfully tested.\(^8\) While institutions were advised to get assurances from outside vendors that their products and services were Year 2000 compliant, management could not rest on those assurances. All electronic products and services provided by outside vendors had to be tested whenever possible in the institution's own environment to ensure that the vendors' systems and the institution's other systems meshed.\(^8\) Management had to specifically ask vendors to explain the scope of testing, the objectives to be attained and the scenarios to be tested. As part of those scenarios, any tests were supposed to simulate and measure the impact of a Year 2000-related disaster on normal operations. Vendors were expected to provide management with testing schedules and failure to do so raised a red flag.\(^8\)

If service providers or software vendors balked at providing sufficient information about their testing efforts, institutions were to complain directly to the suppliers. Institutions were also advised to join forces with other institutions, as part of a user group, to exert collective pressure for adequate information. If problems continued or if laggard suppliers could not meet the institution's target dates, institutions had to activate their remediation contingency plans.\(^8\) In all cases, the appropriate federal regulator had to be notified if problems occurred.\(^8\) Regulators emphasized that the onus was on depository institutions, not on federal examiners, to ensure that vendors were Year 2000 compliant.\(^9\)

\(^8\) See Questions and Answers, supra note 8.
\(^8\) See Project Management Awareness, supra note 12.
\(^8\) See Testing for Year 2000 Readiness, supra note 16; Year 2000 Business Risk, supra note 16.
\(^8\) See Institution Due Diligence, supra note 16; Year 2000 Business Risk, supra note 16.
\(^8\) See id.
\(^8\) See Section III.E.2 infra.
\(^8\) See Questions and Answers, supra note 8.
The Year 2000 project plan also had to provide for testing and verification of electronic data exchanges with correspondent banks, clearing associations, government agencies, customers, credit bureaus, payment system providers, securities firms, international financial institutions and, where possible, phone companies and utilities. The object of those tests was to verify that each institution's network protocol, business applications and operating system platforms worked normally.\textsuperscript{91} FFIEC encouraged depository institutions to participate in joint testing coordinated by industry trade associations and other organizations as a cost-effective way to conduct tests of crucial transactions with other institutions and businesses.\textsuperscript{92} Examples included opportunities by the Federal Reserve System for single-application, end-to-end and shared testing to allow institutions to test systems such Fed Wire and automated clearing house transactions with Fed interfaces, either singly or simultaneously.\textsuperscript{93} Congress shielded joint testing and related communications from antitrust liability in the "Year 2000 Information and Readiness Disclosure Act."\textsuperscript{94}

Questions whether to retest arose where systems that had already been tested underwent later upgrades. The institution was required to ask the service provider or software vendor in question to identify the changes being made and describe the extent to which internal tests were conducted before releasing the upgrade. If the changes did not affect date fields or date-related calculations, the financial institution did not necessarily need to test (other than to perform the routine acceptance testing that would accompany the installation of any software upgrade). Otherwise, the institution had to assure that the upgrade underwent appropriate Year 2000 testing and that the supplier warranted that specific testing was performed to ensure continued Year 2000 readiness.\textsuperscript{95}

\textsuperscript{91} See Testing for Year 2000 Readiness, supra note 16; Project Management Awareness, supra note 12.

\textsuperscript{92} See, e.g., Questions and Answers, supra note 8; Steven Marjanovic, MBA Plans Industrywide Testing Project to Blunt Year-2000 Threat, AM. BANKER, at 8 (Jan. 27, 1998).


\textsuperscript{95} See Questions and Answers, supra note 8.
The last part of the testing process was verification. In this stage, institutions were expected to verify the adequacy of their testing processes and validate their test results. At a minimum, test verification had to involve the institution's Year 2000 project manager, the owner of the system tested and an objective independent party (such as an auditor, a consultant or other qualified individual from within or outside the insured institution who was independent of the process under review). Internal personnel could be used as long as they were qualified and independent of the process being verified. This review was designed to ensure that the tests were effective, that critical dates were checked and that the repairs or upgrades resulted in reliable processing of information. Where an institution relied on proxy testing, management had to ensure that the tests were independently verified. Outside vendors also were required to verify their own tests and supply management with the results.\textsuperscript{96}

E. Contingency Planning

While the goal of Year 2000 repairs and testing was to avoid breakdowns, it was impossible to insure that operations would proceed wholly without interruption. The inability to assure complete Year 2000 readiness in the business world at large was reason enough for lack of assurance. Consequently, federal banking regulators required banks and thrifts to devise thorough contingency plans in case the worst came to pass.

Senior management and the board were charged with overseeing the development and implementation of contingency plans. All contingency plans had to be reviewed at least quarterly and adjusted, if necessary, to reflect changing circumstances. If changes were necessary, those changes had to be approved by senior management and the board. In addition, an independent party (such as an internal or external auditor, a qualified consultant or a qualified person from an independent area within the institution) was supposed to review the contingency plans.\textsuperscript{97}

1. Business Resumption Contingency Plans

The Year 2000 Guidelines required every institution to draft contingency plans for what FFIEC referred to euphemistically as “business resumption” (i.e., business interruption). The requirement for business resumption contingency plans reflected regulators’ lack of total assurance

\textsuperscript{96} See Interagency Guidelines, supra note 17, at 55,485 (1998); Questions and Answers, supra note 8; Testing for Year 2000 Readiness, supra note 16; Project Management Awareness, supra note 12.

\textsuperscript{97} See Questions and Answers, supra note 8; Institution Due Diligence, supra note 16; Year 2000 Business Risk, supra note 16.
that systems would operate as expected, despite the Year 2000 remediation campaign. Such plans addressed the possibility that core business processes might fail, even though an institution was seemingly successful in renovating, testing and implementing Year 2000 readiness. The objective of business remediation contingency plans was to minimize such disruptions to the institution, its customers and business partners, minimize financial losses and ensure a timely resumption of operations in the event a Year 2000 disruption occurred. Unlike remediation contingency planning, which primarily involved information technology specialists reporting to senior management and the board, business resumption contingency planning also required involvement by business personnel outside of information technology.98

Every bank and thrift had to develop and implement an effective written contingency plan designed to accomplish a minimum of three objectives. The plan had to identify and describe the types of scenarios that could be expected if mission-critical systems malfunctioned due to Year 2000 problems. It was required to evaluate possible responses and select a reasonable contingency strategy for the vulnerable systems. Finally, provisions had to be made to test contingency plans, including periodic internal testing, as well as testing by an objective independent party such as an auditor or consultant.99 Contingency plans were required to be appropriate for the institution’s technological systems and operating structures.100 Federal regulators expected the board of directors and senior management to put a high priority on contingency plans.101

There were four phases in the business resumption contingency planning process. All four phases had to be completed by June 30, 1999:102

- Establishing Organizational Planning Guidelines: A key part of developing a business resumption contingency plan was identifying which core business processes might fail if Year 2000 problems were not solved.103 During this phase,
senior management had to designate an individual or working group (possibly including disaster recovery specialists and audit representatives) to develop and monitor the contingency plan. The person or group was responsible for identifying the high priority risks and the functions or processes that needed to work in order for the institution to remain viable. A timeline had to be prepared that allowed sufficient time for testing and activation of the contingency plan, if necessary. Existing contingency plans were to be reviewed to assess their continued effectiveness and eliminate redundancy. A reporting process had to be established to track progress on contingency planning.

Performing A Business Impact Analysis: During this phase, each core business process had to be evaluated for Year 2000 readiness, the financial and marketing impact if that process broke down (including the impact on the very viability of the institution) and the effect of regulatory requirements. This analysis had to consider factors such as the types of risk that could affect core business processes, the likelihood of their occurrence, the probable timing of an occurrence (e.g., quarter end), the cost and duration of operation failure, the impact of multiple system failures, etc. Institutions also had to take into account whether they might experience unusual funding needs in late 1999 and early 2000 arising from surges in deposit outflows or loan demands.\textsuperscript{104} Priority went to possible failures that would have had the worst effect on the institution's core business processes. Year 2000 failure scenarios had to be developed to pinpoint the types and levels of business needs that had to be met.

Developing A Business Resumption Contingency Plan: Armed with the results of the business impact analysis, the institution was required to investigate contingency options

\textsuperscript{104} In such an event, normal liquidity sources had to be expanded and alternative sources located. Institutions that had to rely on the Federal Reserve's discount window due to lack of market funding sources were advised to file the appropriate documents and pledge collateral as early as possible in 1999. Thrifts that were members of the Federal Home Loan Bank System could also have requested advances. \textit{See Questions and Answers, supra} note 8.
and select strategies that were cost-effective and most reasonable, given the institution's size, complexity and type of information systems used. The primary goal of the contingency plan was to maximize the operating capability and speed of recovery. The plan had to contain a recovery plan for each core business process that would result in at least a minimum level of acceptable service. Consideration had to be given to quick fixes, partial replacement or reliance on other manual or automated processes. FFIEC announced that branches could be temporarily closed due to Year 2000 disruptions beyond an institution's control without being subject to the normal branch closing procedures in 12 U.S.C. § 1831r-1. As part of the contingency plan, a crisis management team needed to be designated and made responsible for implementing the plan and responding promptly to reaction from customers and the media. Management had to consider how to respond to events outside of the institution's control that could substantially affect customer confidence. All members of the crisis management team were required to receive appropriate training to carry out the contingency plan. Realistic trigger dates for activating the plan had to be set. Sufficient staff had to be on hand to handle any disruptions between December 30, 1999 and January 3, 2000, as well as on other key dates.

Copies of all key data and files had to be made, either in hard copy or machine-readable form. Where an institution relied on systems provided by third parties, it had to take account of the outside vendors' contingency plans. Legal counsel were advised to review data processing and other vendor contracts where necessary to determine each party's responsibility. Data processing insurance coverage had to be reviewed and a public relations committee established to ensure accurate public statements. The feasibility of the contingency plan had to undergo an independent review by qualified individuals, such as internal or external auditors or employees who were not involved in formulating the plan.

Institutions, in consultation with counsel, were advised to consider any applicable state law requirements regarding branch closings and the effect of other obligations regarding provision of services to affected customers. See Questions and Answers, supra note 8.
Designing Validation Methods: The staff who were responsible for the contingency plan were required to stay abreast of the institution's progress under its overall Year 2000 plan and adjust the contingency plan accordingly to reflect any changes. The contingency plan had to be periodically tested through methods such as simulations, role play, walk-throughs and alternate site reviews.

As part of a business resumption contingency plan, management was responsible for considering how the institution might be vulnerable if outside vendors failed to meet their contractual service obligations due to Year 2000 problems. Alternate service or software providers needed to be identified in case vendors' attempts at Year 2000 compliant repairs or upgrades proved inadequate. Trigger dates for hiring those alternate providers had to be set and put into effect where necessary. Management was required to consult legal counsel about available legal remedies or strategies in such an event and notify federal regulators of any such difficulties.

Federal regulators expected contingency plan provisions on service providers and software vendors to contain the following components:

1. A risk assessment that identified potential disruptions and the effect those disruptions could have if a service provider or software vendor was unable to achieve Year 2000 compliance. The risk assessment had to evaluate the probability of such disruptions and devise controls to minimize, eliminate or respond to that risk.

2. Analysis of available strategies and resources to restore system or business operations.

3. A recovery program that identified the internal and external personnel, processes and equipment that were necessary for the institution to function at an adequate level. All of the participants had to be aware of their roles and have adequate training.

4. A comprehensive schedule of each vendor's remediation program, including trigger dates. Institutions were advised to build in additional time for repairs if internal test results failed.

See Project Management Awareness, supra note 12.

See Institution Due Diligence, supra note 16.

See id.
2. Remediation Contingency Plans

A second type of contingency plan, called a remediation contingency plan, was required for institutions that had not successfully completed repairs, testing and/or implementation, or that had fallen behind schedule in accomplishing those tasks. A formal written remediation contingency plan was not required for mission-critical systems or applications that had been successfully remediated, tested and implemented. If an institution or any of its service providers or outside software vendors were unable to complete repairs, testing and implementation successfully within federal deadlines, then a written remediation contingency plan was needed.

All such institutions were required to develop and implement an effective written remediation contingency plan that satisfied a minimum of two objectives. First, the plan had to outline the available alternatives if repairs, testing and implementation did not succeed (such as resort to other third party suppliers) and select a reasonable contingency strategy. Second, the plan had to establish trigger dates for activating the plan, taking into account the time that would be needed to switch to outside suppliers or to complete any other chosen strategy. Such contingency plans were key for products and services provided by vendors that were mission-critical.

Where payment of a fee was necessary to ensure that an alternative service provider or vendor was available, whether to pay the fee was a business decision that the board of directors and senior management were required to make. In arriving at that decision, the board and management had to consider the probability that Year 2000 readiness efforts might fail, either on the part of the institution or existing service providers or software vendors. Management and the board also had to take into account the extent to which existing providers had met the institution’s timetable, the amount of time needed to switch to alternate providers, the availability of such providers and their reputation among other institutions or user groups.

---

109 See Questions and Answers, supra note 8.
110 See Interagency Guidelines, supra note 17, at 55,485.
111 See Year 2000 Business Risk, supra note 16.
F. Implementation

During the implementation phase, banks and thrifts were required to tackle several tasks. First and foremost was addressing systems that did not pass testing. It was imperative that any mission-critical systems that were still not compliant immediately be brought to the attention of top management. For systems that failed testing, the business consequences had to be assessed and the contingency plan for that system had to be put into effect. For complex applications whose success was in doubt, it was necessary to implement the contingency plan while continuing to work on a solution. Where replacement systems could not be installed in time, existing systems had to be repaired.\(^\text{113}\)

During implementation, staff also had to be trained to operate upgrades and any new systems. It was important to allocate sufficient time for training.\(^\text{114}\)

Attention also had to be paid to computerization purchases down the road. Management was required to verify that any new systems or subsequent changes to compliant systems were Year 2000 compliant.\(^\text{115}\)

G. Response To Customer Inquiries

As the Year 2000 approached, customers looked to banks and thrifts for assurances that their institutions would not experience service disruptions due to the century date change. In an effort to stem public panic and alarm, federal regulators stressed the importance of devising “customer awareness programs” designed to respond to questions and communicate with customers about Year 2000 issues. Management and the board of directors were ultimately responsible for making certain that customers received satisfactory responses to their Year 2000 concerns.\(^\text{116}\)

Many customers were concerned about the safety of the funds in their accounts. News accounts advised depositors to withdraw cash, prompting customers to ask whether they should withdraw cash and, if so, how much.\(^\text{117}\) The ability to access funds through ATMs, debit cards, phone

\(^{113}\) See Year 2000 Business Risk, supra note 16; Project Management Awareness, supra note 12.

\(^{114}\) See Year 2000 Business Risk, supra note 16.

\(^{115}\) See Project Management Awareness, supra note 12.

\(^{116}\) See Customer Awareness Programs, supra note 16.

\(^{117}\) In anticipation of stepped-up withdrawals, the Federal Reserve System ordered enough new currency notes to boost printing of currency notes thirty-three percent. See Susan McInerney, Fed, Treasury Bulk Up Cash Reserves to Meet Year 2000 Currency Demands, 71 BNA BANKING REP. 251 (1998).
lines or the Internet was also of concern and institutions had to offer alternate means of access if disruptions occurred.

Similarly, institutions were advised to expect questions about the reliability of direct deposit, direct debit and other automatic electronic payments. Institutions were instructed to explain how they would assist customers if automatic transactions went haywire. Borrowers worried about receiving proper credit for loan payments. Customers asked what types of records they should maintain before and after January 1, 2000. They also requested general information about the institution’s record keeping practices and the status of its Year 2000 efforts and contingency plans.118

Institutions were expected to take the initiative to inform customers such as depositors, borrowers, fiduciary clients and others who transacted business with them about their Year 2000 readiness. Consideration had to be given to notifying customers through brochures or inserts accompanying monthly statements, toll-free hotlines, seminars or web site disclosures.119 Legal counsel were advised to review any disclosures in advance.120

In addition, personnel who regularly interacted with customers had to be trained to respond appropriately to inquiries by providing customers with written information or referring them to expert staff. Institutions were encouraged to disseminate news of their Year 2000 programs to news media and community organizations.121

In February 1999, FFIEC issued a guidance on the elements that customer communications statements should address.122 Because customers could be confused about the nature of the Year 2000 problem, banks and thrifts had to explain what the Year 2000 problem was. Regulators stressed that customers should be informed “up-front that maintaining their confidence in banking with the financial institution—now and after the Year 2000—was a top priority.”123 Customers were to be given assurances that the institution would have contingency plans in place to ensure that customers had access to their money and accurate account information in

118 See Customer Awareness Programs, supra note 16.
119 See id. The FDIC developed two publications that institutions distributed to customers. The first was entitled “The Year 2000, Your Bank and You.” In addition, the FDIC developed a Year 2000 “statement stuffer” for inclusion with monthly statements. See FDIC, Two New FDIC Publications for Consumers on the Year 2000 Problem, FIL-137-98, 1998 FDIC Interp. Ltr. LEXIS 126 (Dec. 30, 1998).
120 See Customer Awareness Programs, supra note 16.
121 See id.
123 See id.
case problems occurred. In addition, institutions were told to point out that accounts were covered by $100,000 in federal deposit insurance. They were similarly urged to describe the institution's progress toward its Year 2000 plan and emphasize the involvement of senior management as well as federal and state regulators.\footnote{See id.}

When making disclosures, banks and thrifts had to be careful to avoid public disclosures of information or summary ratings from Year 2000 examinations or reviews, whether that information related to the institution, outside service providers or software vendors.\footnote{See Customer Awareness Programs, supra note 16; Section V.A infra.} Banks and thrifts also had to avoid any statements that might give the impression that regulators had approved or certified their Year 2000 readiness.\footnote{See Customer Awareness Programs, supra note 16.}

Customer confidence was not simply a matter of public relations. Banks and thrifts could have offered financial inducements to keep customer accounts. For instance, banks could have considered offering free checking for deposits over a certain level to encourage depositors not to withdraw funds. Institutions could also have considered providing Year 2000 demonstrations to show customers how their accounts might be affected by the Year 2000 date change.\footnote{See Year 2000: Computer Glitch Presents Opportunities, Risks for Banks and Thrifts, Expert Says, 71 BNA BANKING REP. 681 (1998).}

**H. Obligations Of Management And The Board of Directors**

Above all, federal banking regulators looked to an institution's board of directors and management to ensure compliance with the Guidelines and Year 2000 readiness. The Year 2000 Guidelines and guidances placed a heavy onus on managers and directors and required active intervention and monitoring by management and the board.

Under the Guidelines, management and the board could not turn over Year 2000 compliance to a project manager and then sit back. During all stages of repairs, testing and contingency planning, management and the board had to actively oversee planning, resource allocation, and the institution's progress toward Year 2000 readiness.\footnote{Thomas Vartanian developed a valuable checklist for board and management oversight. See Thomas P. Vartanian, Year 2000 compliance checklist, BUS. L. TODAY 45 (Sept./Oct. 1998).} Together, both bodies were expected to allocate sufficient resources to successfully resolve any Year 2000 problems. Senior management was expected to manage the Year 2000 project on a day-to-day basis.\footnote{See Interagency Guidelines, supra note 17, at 55,485.} If the institution was contemplating

\footnotesize{124 See id.} \footnotesize{125 See Customer Awareness Programs, supra note 16; Section V.A infra.} \footnotesize{126 See Customer Awareness Programs, supra note 16.} \footnotesize{127 See Year 2000: Computer Glitch Presents Opportunities, Risks for Banks and Thrifts, Expert Says, 71 BNA BANKING REP. 681 (1998).} \footnotesize{128 Thomas Vartanian developed a valuable checklist for board and management oversight. See Thomas P. Vartanian, Year 2000 compliance checklist, BUS. L. TODAY 45 (Sept./Oct. 1998).} \footnotesize{129 See Interagency Guidelines, supra note 17, at 55,485.}
any strategic business transactions, such as mergers and acquisitions, major
systems development, corporate alliances or system interdependencies,
management and the board had to evaluate the Year 2000 risk associated
with those transactions.\textsuperscript{130} The first issue was whether the institution’s
internal audit function and internal controls were up to the task of keeping
tab on progress toward Year 2000 compliance.

Management also had to ensure that sufficient internal controls were
in place to make certain that the institution stayed on schedule with Year
2000 remediation.\textsuperscript{131} As part of its oversight responsibilities, every
institution’s board of directors had to require management to provide it with
written status reports on Year 2000 readiness. Management had to furnish
those reports to the board at least quarterly and keep the board otherwise
informed of the progress toward Year 2000 compliance. The status reports
had to discuss the institution’s overall progress in attaining readiness and
progress to date compared with the projected completion dates in the
institution’s Year 2000 plan. Status reports also had to discuss progress or
lack thereof by key outside vendors in providing Year 2000 compliant
services, as well as progress by other material third parties (such as
correspondent banks and check clearing houses) in achieving Year 2000
readiness. Material customers who were not effectively addressing their own
Year 2000 problems had to be brought to the board’s attention at least
quarterly and actions to control such risks had to be discussed. Special
attention also had to be paid to internal and external testing results, the status
of contingency planning and the status of customer risk assessments.\textsuperscript{132}

If the Year 2000 project failed to meet critical benchmarks, the board
was to be notified immediately.\textsuperscript{133} Because examiners inspected board
minutes for evidence of active oversight by the board, the minutes needed to
reflect all material actions by the board to address Year 2000 issues or
concerns.\textsuperscript{134}

IV. BROADER BUSINESS ISSUES

Federal banking regulators conditioned the approval of applications
for branching, mergers and acquisitions, etc., on satisfactory progress toward

\textsuperscript{130} See id.; Section III.B infra.
\textsuperscript{131} See Project Management Awareness, supra note 12.
\textsuperscript{132} See Interagency Guidelines, supra note 17, at 55,485; Year 2000 Impact on
Customers, supra note 16; Year 2000 Business Risk, supra note 16.
\textsuperscript{133} See Year 2000 Business Risk, supra note 16.
\textsuperscript{134} See Year 2000 Business Risk, supra note 1; Project Management Awareness,
supra note 12.
Year 2000 readiness. The Year 2000 problem also posed important accounting and financial disclosure issues, both under generally accepted accounting principles and the federal securities laws.

The Year 2000 problem was not solely an issue of technology or repairs. As federal regulators repeatedly stressed, the Year 2000 problem had consequences for everything from loan underwriting and strategic business alliances to financial disclosures and bottom-line profitability. Management needed to take account of these broader ramifications of the Year 2000 problem.135

A. Mergers, Acquisitions And Other Regulatory Applications

Integrating computer systems during mergers or acquisitions is complex and fraught with problems during the best of times, and these problems intensified with the added pressure of Year 2000 readiness.136 As already discussed, federal regulators expected every institution, during its Year 2000 assessment process, to consider the potential effects that mergers and acquisitions, major system development, corporate alliances and system interdependencies could have had on the Year 2000 readiness of affected computer systems, both for existing systems and any that were acquired.137 In addition, regulators conditioned the approval of applications (whether those applications were limited to branching or sought approval of mergers or acquisitions) to successful handling of the century date change.138

In 1998, the Comptroller of the Currency issued an advisory letter in which he announced that OCC approval of corporate applications (including applications for charters, conversions, business combinations, branching and establishment of operating subsidiaries that would rely heavily on technology) would depend on Year 2000 preparedness and the ability to integrate hardware and software systems resulting from any proposed

135 See Year 2000 Business Risk, supra note 16.
137 See Interagency Guidelines, supra note 17, at 55,485; Project Management Awareness, supra note 12.
In that regard, the OCC specifically looked for compliance with the Year 2000 deadlines set by regulators and the safety and soundness guidelines and guidances on the Year 2000 problem. Where Year 2000 deficiencies became apparent upon review, expedited processing could be denied. Additionally, the OCC could condition approval on remedial actions or deny applications altogether.140

Similarly, the Federal Reserve Board of Governors required applicants for mergers or acquisitions to show that the transactions would not impede Year 2000 readiness.141 Banking organizations with less-than-satisfactory Year 2000 ratings did not qualify for expedited processing and were instructed to advise Federal Reserve officers before deciding to embark on any activity requiring federal approval, including acquisitions or expansion.142 Applicants were expected to demonstrate Year 2000 readiness, as well as sufficient financial and managerial resources to ensure compliance throughout the combined or expanded organization. The Federal Reserve looked with disfavor on any proposed expansion that diverted resources needed to ensure Year 2000 readiness. In order for applicants with less-than-satisfactory Year 2000 ratings to obtain approval by the Fed, the Fed had to conclude that the applicant’s Year 2000 rating could be upgraded to satisfactory or that the proposal would have no material bearing on the applicant’s ability to meet its Year 2000 responsibilities, e.g., due to the limited nature of the proposal.143 The Fed announced in that regard that banks that were too far behind in Year 2000 readiness could not expect to remedy the problem by putting themselves up for sale. According to the Fed,

---

140 See id.
143 See SR Letter 98–3, supra note 142.
that approach "[was] a high risk, unacceptable plan of action" that the Fed refused to countenance.\footnote{144}{See id.}

In late 1998, the Federal Reserve Board proposed amending Regulation CC to lengthen the normal one-year transition period for merged banks to integrate their computer systems. The proposal applied to banks that consummated mergers between July 1, 1998 and June 1, 1999. Under the proposal, the Fed treated those banks as separate banks until June 1, 2000, whereupon the one-year transition period would begin to run. The purpose of the proposed amendment was to allow bank mergers to proceed without concern that mandatory system integration would divert resources that were better put to use toward Year 2000 readiness.\footnote{145}{See Federal Reserve Rulemaking Release, Regulation CC, Docket No. R–1027 (Dec. 23, 1998); Availability of Funds and Collection of Checks, 63 Fed. Reg. 66,499 (1998).}

B. Financial Reporting And Disclosure

The Year 2000 problem had major financial and reporting consequences that needed to be addressed by management. From the perspective of safety and soundness, federal banking regulators expected management to assess the effect of Year 2000 repairs on an ongoing basis on earnings, capital and liquidity.\footnote{146}{See Project Management Awareness, supra note 12.} Parallel obligations appeared in the new federal securities disclosure requirements for publicly held banking organizations.

those requirements to publicly traded banks and bank holding companies. In addition, the FDIC recommended that other institutions make disclosures on Year 2000 readiness either in the annual disclosure statements required of FDIC-insured institutions under 12 C.F.R. pt. 350, in their annual reports to shareholders or, where applicable, in the annual reports required of institutions with a half-billion dollars or more in assets under 12 C.F.R. pt. 363.

Under the SEC’s interpretation, a publicly held company had to provide Year 2000 disclosures if (1) its assessment of its Year 2000 issues was not complete, or (2) management determined that the consequences of its Year 2000 issues would have a material effect on the company’s business, results of operations, or financial condition, without taking into account the company’s efforts to avoid those consequences. Under the first prong, the company had to verify the Year 2000 readiness of any third party who could have a material impact on the company. Relevant third parties included vendors and suppliers who could have a material effect on the company’s business if they did not achieve compliance; customers whose lack of Year 2000 readiness could cause a material loss of business; and other third parties to whom the business might be legally liable for any Year 2000 business disruptions.

Under the second, alternative prong of the test for disclosure, the SEC advised that companies should normally assume that they and their material third-party suppliers and customers were not Year 2000 compliant for purposes of securities disclosures (absent clear proof to the contrary) and should therefore make disclosures weighing the likely results of that lack of preparedness. The balancing test was to be conducted by calculating the consequences if the company was not prepared, rather than the amount of money the company planned to spend to address Year 2000 issues. Uncertainties relating to remediation, business relationships with third parties, business interruptions, litigation, insurance and other contingencies had to be taken into account.

---


150 See SEC Interpretation, supra note 147.

151 See id.

152 See id. In determining whether potential Year 2000 consequences were material, the company could have excluded any quantifiable dollar amounts whose risks were covered by Year-2000-specific insurance policies. See id.
its testing and assessment of third party issues, obtained written representations of preparedness by all material third parties and thus had a reasonable basis to assume that it was Year 2000 ready, it was not obliged to make disclosures under prong two. Nonetheless, the SEC advised disclosure in any case.\textsuperscript{153} The SEC expected that "for the vast majority of company Year 2000 issues [were] likely to be material and therefore disclosure [was] required."\textsuperscript{154} Furthermore, because new Year 2000 issues almost always cropped up as a company worked through remediation, the SEC expected companies to update their Year 2000 disclosures in each of their quarterly and annual reports.\textsuperscript{155}

Where a bank, bank holding company or nonbank affiliate had a Year 2000 disclosure obligation, the SEC expected the company to make disclosures on the following topics in the Management Discussion and Analysis ("MD&A") sections of their quarterly (10Q) and annual (10K) reports:\textsuperscript{156}

- \textit{The Company's State Of Readiness:} The company was required to describe its Year 2000 issues in sufficient detail so that investors could understand the challenges that the company faced. The discussion was to address both information technology systems and environmental systems, such as elevators and vaults, that had embedded technology such as microcontrollers. The company was required to describe its progress to date in each of the phases of remediation (awareness, assessment, repairs, testing, implementation and contingency planning) and whether the company was on schedule. On the topic of testing, serious consideration was to be given to disclosing what kinds and percentage of the company's hardware, software and embedded systems had been tested and validated as Year 2000 ready and what testing and verification methodologies were used. The Year 2000 issues raised by the company’s material business relationships with outsiders also needed to be disclosed. The OCC took the position that any informal

\begin{footnotesize}
\begin{enumerate}
  \item See id.
  \item Id.
  \item See id.
  \item See id.
\end{enumerate}
\end{footnotesize}
and formal enforcement actions regarding Year 2000 issues against the company also triggered disclosure to the SEC.\textsuperscript{157}

\begin{itemize}
  \item \textbf{The Costs Of Addressing The Company’s Year 2000 Issues:} The SEC expected the material historical and estimated costs of remediation to be disclosed. The cost of replacing non-compliant systems had to be disclosed except in unusual cases where the company would have replaced the systems anyhow and did not accelerate replacement due to Year 2000 issues.\textsuperscript{158}
  \item \textbf{The Risks Presented By The Company’s Year 2000 Issues:} Companies were required to include a reasonable description of their most reasonably likely worst case Year 2000 scenario. Unless the company was certain that this scenario would not be likely to have a material effect on the company’s results of operations, liquidity and financial condition, any uncertainty had to be disclosed, as well as efforts to analyze and handle this uncertainty.
  \item \textbf{The Company’s Contingency Plans:} Companies were required to describe how they would handle the most likely worst case scenarios. They had to describe their contingency plans or their progress toward adopting contingency plans, if none yet existed.
\end{itemize}

Companies also had to disclose any other material matters that circumstances dictated.\textsuperscript{159}

Companies were instructed to consider the proper accounting and auditing treatment of Year 2000 issues when preparing their financial statements. Special attention needed to be given to the treatment of Year-2000 related payment commitments, acceleration of loans due to Year-2000

\begin{flushright}
\textsuperscript{158} The SEC also urged disclosure of other matters relating to costs, including: all Year-2000 related costs, even if those costs were not material; how much of total estimate Year 2000 project costs had already been incurred at the end of each reporting period; the source of funds for Year 2000 costs, including the percentage of the information technology used for remediation; whether other information technology projects had been deferred due to Year 2000 efforts and the effects of this delay on financial condition and results of operations; any independent verification and validation process used to assure the reliability of risk and cost estimates, particularly during testing; a chart tracking the company’s Year 2000 progress over time; and a breakdown of the costs incurred to achieve Year 2000 readiness. See SEC Interpretation, \textit{supra} note 147.
\textsuperscript{159} See id.
\end{flushright}
related defaults, loan loss provisions and revenue and loss recognition.\textsuperscript{160} It was important not to ignore the fact that Year 2000 repairs or new systems could inadvertently introduce changes that affected or impaired an institution's accounting system and/or internal controls.\textsuperscript{161}

In the interpretive release, the SEC took the position that the statutory safe harbors for forward-looking information under the 1933 and 1934 Acts\textsuperscript{162} applied to numerous MD&A disclosures on Year 2000 readiness. MD&A projections of future costs were forward-looking statements, as were descriptions of contingency plans, statements of readiness based on third-party representations, anticipated Year 2000 problems and future timetables. However, statements of historical fact, such as descriptions of past efforts at Year 2000 readiness (or lack thereof), did not merit protection.\textsuperscript{163} In addition, for the statutory safe harbors to apply, material forward-looking statements had to be accompanied by "meaningful cautionary statements," none of which could be boilerplate or knowingly false when made.\textsuperscript{164}

It is important to note that the statutory safe harbors did not apply to initial public offerings or to investment companies. The same was true for statements included in financial statements prepared in accordance with generally accepted accounting principles.\textsuperscript{165} Thus, statements of estimated costs that were included in MD&A disclosures outside of the financial statements were immune from suit, but inclusion of those costs in the financial statements themselves or discussion of those costs in footnotes to the financial statements were not protected.\textsuperscript{166}

V. AGENCY SUPERVISION AND ENFORCEMENT

Beginning in 1997, federal banking regulators examined insured banks and thrifts for their progress toward Year 2000 readiness. Where institutions' compliance ratings were less than satisfactory, agencies pursued formal enforcement actions, including cease-and-desist orders and civil money penalties, in order to avoid systemic problems due to Year 2000 malfunctions.

\begin{itemize}
\item \textsuperscript{160} See id. See generally American Institute of Certified Public Accountants, \textit{The Year 2000 Issue: Current Accounting and Auditing Guidance} (1998) for a discussion of the accounting and auditing treatment of Year 2000-related issues.
\item \textsuperscript{161} See \textit{Year 2000 Business Risk}, supra, note 16.
\item \textsuperscript{162} 15 U.S.C. §§ 77z–2, 78u–5.
\item \textsuperscript{163} See SEC Interpretation, supra note 147.
\item \textsuperscript{165} See 15 U.S.C. §§ 77z–2(b), 78u–5(b).
\item \textsuperscript{166} See SEC Interpretation, supra note 147.
\end{itemize}
The banking industry’s success in achieving Year 2000 readiness can partly be attributed to the fact that federal regulators made it clear beginning in 1997 that they would take vigorous enforcement against institutions that failed to take appropriate steps toward Year 2000 compliance. Regulators made good on their word.

A. Examinations

In 1998, federal banking regulators undertook Phase I of their special on-site examinations for Year 2000 readiness. That first round, which was completed on June 30, 1998, sought to evaluate the awareness and assessment activities of all insured banks and thrifts. As of year-end 1998, approximately three percent of banks examined had received less-than-satisfactory ratings.

Phase II of the Year 2000 examinations was scheduled to be completed on March 31, 1999. The purpose of the second-round examinations was considerably more searching and was intended to verify that mission-critical systems had been repaired or upgraded and tested and that contingency plans were in place. Highest priority was given to the large financial institutions that present the greatest degree of national or regional systemic risk, as well as to institutions that had previously been identified as less than satisfactory and the largest service providers and software vendors.

Phase III of the Year 2000 examinations commenced immediately after completion of Phase II. In Phase III, federal examiners reviewed the efforts of depository institutions and their outside suppliers to comply with federal guidelines and deadlines for testing, implementation and contingency planning. Once again, priority was given to the largest institutions with

---


168 See Brett Chase, Mellon Works with Vendors, Customers in Run-Up to 2000, AM. BANKER 5 (Feb. 3, 1999); Letter from Comptroller of the Currency John D. Hawke, Jr., to Chief Executive Officers of National Banks, at 1 (Feb. 17, 1999).

assets over $1 billion, suppliers who presented the greatest degree of risk, and institutions and suppliers previously ranked as less than satisfactory.\textsuperscript{170}

During the first round of examinations, the Federal Reserve Board unveiled its supervisory rating system for Year 2000 compliance.\textsuperscript{171} Other federal banking regulators adopted the Fed's ranking system as a matter of practice. Under that system, an institution could receive one of three ratings: satisfactory, needs improvement or unsatisfactory. Anything less than a satisfactory rating could cause the institution's overall safety and soundness rating to fall or subject the institution to intensified scrutiny by regulators.\textsuperscript{172}

A "satisfactory" rating was warranted when project weaknesses were minor in nature and could readily be corrected within the existing project framework. To issue a "satisfactory" rating, examiners looked for assurances that senior management and the board understood the Year 2000 risk, were active in overseeing institutional corrective efforts, and devoted sufficient resources to solving the problem.\textsuperscript{173}

A "needs improvement" rating meant that the institution showed less than satisfactory performance in any of the key phases of the Year 2000 project management process. Failure to adhere to Year 2000 time lines would result in a "needs improvement" rating. The same was true where senior management or directors were not fully apprised of Year 2000 corrective efforts, had not committed sufficient financial or human resources to address the risk, or did not fully understand Year 2000 implications. Examiners specifically scrutinized whether any key elements in the Year 2000 Guidelines or the FFIEC guidances had not been addressed. A poor response to potential Year 2000 problems of vendors could also lead to a "needs improvement" rating.\textsuperscript{174}

An "unsatisfactory" rating showed critical deficiencies and poor performance in any of the key phases of the Year 2000 program. In unsatisfactory institutions, project weaknesses were serious and were not easily corrected within the existing project management plan. The institution's progress was seriously behind schedule. Senior management and the board underestimated the potential impact that the Year 2000

\textsuperscript{172} See id.
\textsuperscript{173} See id.
\textsuperscript{174} See id.
problem could have on their institution, had limited commitment to fixing the problem and failed to exercise oversight.

An "unsatisfactory" rating was warranted where due diligence as to outside suppliers was seriously flawed or where the institution had not addressed the credit risks associated with the Year 2000 problem with respect to large borrowers or bond issuers.175

A variety of lapses could result in less-than-satisfactory ratings on Year 2000 examinations. Prime among them were inadequate contingency plans (particularly with respect to vendors), failure to complete assessment, inadequate project plans, insufficient audit coverage of the institution's Year 2000 progress, insufficient vendor evaluations and failure to evaluate the Year 2000 readiness of major customers.176

Insured institutions were not the only entities that were subject to federal Year 2000 examinations. Under existing statutory authority, the FDIC, OCC and Federal Reserve Board had power to examine outside service providers and software vendors for banks for Year 2000 readiness. In 1998, President Clinton signed into law the Examination Parity and Year 2000 Readiness for Financial Institutions Act,177 which granted identical examination and enforcement powers to the Office of Thrift Supervision and the National Credit Union Administration.178

The federal bank regulatory agencies insisted that Year 2000 examination reports and results from those reports remain confidential and not be disclosed to the general public.179 The fear was that otherwise, banks with satisfactory ratings would tout those ratings to the public as proof of their Year 2000 readiness, when that might not have been the case. This injunction applied to all Year 2000 examination reports, whether those examinations were of depository institutions, service providers or software vendors. Financial institutions, service providers and software vendors were also specifically forbidden from stating or implying that their Year 2000 plans or readiness had been approved or certified by regulators.180

B. Enforcement

As early as May 1997, federal banking regulators announced that they would take enforcement action against institutions that persistently

175 See id.
178 Id. § 3.
180 See Questions and Answers, supra, note 8.
failed to pay adequate attention to Year 2000 compliance. Enforcement measures could range from deficiency letters at a minimum to civil money penalties or worse.

The OCC announced in early 1999 that for banks with less-than-satisfactory ratings, the agency would henceforth rely primarily on the deficiency letter process and less on supervisory directives and other informal enforcement. A deficiency letter listed specific potential problems that a bank or thrift needed to address. Banking organizations with less-than-satisfactory progress could also have been placed on intensified monthly monitoring which required them to submit monthly progress reports to their primary federal banking regulator. Institutions could have also received lower examination ratings for risk management or overall management or conditions because of Year 2000 deficiencies.

Authority for deficiency letters was found in the safety and soundness standard provisions of 12 U.S.C. § 1831p-1. Under that provision, federal banking regulators were authorized to issue deficiency letters requiring institutions that failed to comply with the Year 2000 Guidelines to submit an acceptable compliance plan within thirty days of a request. If such a plan was not submitted on time or turned out to be unacceptable, the agency had to issue an order directing the institution to correct the deficiency. Such orders were enforceable in federal district court, with no need for prior agency adjudication. Violation of such orders provided the basis for assessing civil money penalties against institutions and institution-affiliated parties, including officers and directors. The Federal Reserve Board announced that any banking organization within its jurisdiction that had not submitted an acceptable corrective plan within thirty

---

181 See Project Management Awareness, supra note 12.
184 See id.
187 Id. § 1818(i); 12 C.F.R. § 30.6, 263.305, 308.305, 570.5.
188 Id. § 1818(i)(2); 12 C.F.R. § 30.6, 263.305, 308.305, 570.5.
days of receiving a Year 2000 deficiency letter faced immediate formal enforcement.  

Receipt of a deficiency letter did not preclude formal enforcement action, such as a cease-and-desist order, a removal or prohibition order, or a civil money penalty. The agencies reserved the right to take any other enforcement measures that were appropriate to insure Year 2000 readiness. Institutions that planned to apply to federal regulators for expansion through branch openings or mergers and acquisitions were warned that they would be turned down unless they had made satisfactory progress toward the century date change. At an extreme, regulators had the power to close non-compliant institutions.

Not satisfied with the deficiency letter process alone, the Federal Reserve Board raised the heat when it announced that in 1999, any banking organization rated less than satisfactory “for serious violations of the FFIEC’s Year 2000 compliance standards [would] be subject to public formal enforcement actions.” The Board was particularly concerned that noncompliance at such a late date “could with some certainty affect the organization’s readiness for the millennium rollover.” In less serious cases, where institutions received “needs improvement” ratings for infractions that were less than significant, the Fed pursued informal enforcement in the form of a memorandum of understanding or board resolution.

Cease-and-desist orders were the most common type of formal enforcement action. To add urgency to the need for Year 2000 readiness, federal banking regulators began imposing cease-and-desist orders (normally on a consent basis) in late 1997 for Year 2000 violations with increasing regularity. Cease-and-desist orders were issued against banks and bank

---

191 See Interagency Guidelines, supra note 17, at 55,482, 55,484; 12 U.S.C. §§ 1831p–1(e)(2), (e)(3); 12 C.F.R. §§ 30.4(d), 263.303(d), 308.303(d), 570.3(d).
194 Id.
195 See id.
196 See, e.g., Board of Governors of the Federal Reserve System, Announcement H2, 1999 No. 5 (Jan. 30, 1999) (written agreement with First Utah Bank in Salt Lake
holding companies for apparent failures to complete a Year 2000 plan or initiate repairs, inadequate Year 2000 project plans or resources, failures to test renovated systems by federal deadlines, failures to designate a senior manager responsible for overseeing Year 2000 readiness, failures to evaluate large borrowers’ Year 2000 compliance efforts, and inadequate

\[\text{City, Utah, to help ensure Year 2000 readiness) (discussed in Fed, Utah Bank Agree on Year 2000 Guidelines, BNA BANKING REP. 349 (Feb. 22, 1999)}.\]


testing. Federal regulators also entered cease-and-desist orders against data service providers to banks for lack of Year 2000 preparedness. In addition, Year 2000 compliance clauses became routine in cease-and-desist orders against institutions that were unsafe or unsound in other respects. The Federal Reserve Board further advised Federal Reserve Banks to issue temporary cease-and-desist orders whenever "necessary to immediately remedy severe Year 2000 deficiencies.

In early 1999, the Federal Reserve Board advised that civil money penalties, removal or prohibition should be invoked against banking organizations that were in "substantial noncompliance with a written agreement or cease and desist order addressing Year 2000 problems." Any Reserve Bank that failed to institute such measures in cases involving


206 Id.
substantial noncompliance had to provide written justification to the Director of the Division of Banking Supervision and Regulation.\textsuperscript{207}

VI. EPILOGUE

This chronicle ends in the spring of 1999, when federal Year 2000 enforcement efforts were at their height and institutions were in the throes of Year 2000 testing. In the final analysis, the story ended happily, but its meaning was unclear. On January 1, 2000 and during the weeks thereafter, virtually no Year 2000 problems of any significance were reported at United States banks and regulators and the public breathed a collective sigh of relief. Other industries outside of the financial services industry achieved identical success, however, through voluntary compliance. Thus, it is premature to say whether the costly system of command-and-control regulation in the banking industry was a resounding success or simply regulatory overkill. The Year 2000 episode and the different enforcement regimes that ensued deserve further study as a valuable laboratory for diverse regulatory approaches to a common problem.

\textsuperscript{207} See id.