

Y2K



Office of Inspector General



March 24, 2000
Audit Report No. 00-012

**Special Report: FDIC's Year 2000
Efforts**





DATE: March 24, 2000

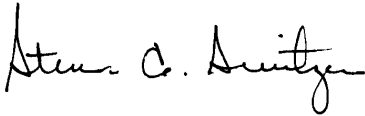
TO: John F. Bovenzi
Deputy to the Chairman and Chief Operating Officer

Donald C. Demitros
Director
Division of Information Resources Management and Chief Information Officer

James L. Sexton
Director
Division of Supervision

Mitchell Glassman
Director
Division of Resolutions and Receiverships

Arleas Upton Kea
Director
Division of Administration



FROM: Steven A. Switzer
Deputy Inspector General

SUBJECT: Special Report on FDIC's Year 2000 Efforts (Audit Report No. 00-012)

Beginning in February 1997, the Office of Inspector General (OIG) engaged in a comprehensive assessment of the Federal Deposit Insurance Corporation's (FDIC) efforts to ensure year 2000 (Y2K) readiness of both the financial institutions that it supervises and its internal systems. As a result of vigorous actions taken by the Corporation, the FDIC successfully transitioned to the new millennium. During the rollover weekend and to date, the banking institutions supervised by the FDIC have experienced no major disruptions, and the Corporation's internal operations have continued uninterrupted. Although the Corporation's Y2K efforts continue, the majority of the Corporation's work is complete. We are issuing this special report following the culmination of our Y2K audit efforts on March 7, 2000.

This report primarily focuses on the positive actions undertaken by the Corporation in addressing the uncompromising and unprecedented technological challenge posed by the date change to the year 2000. The OIG believes that the Corporation would be well served if many of the initiatives

implemented to address Y2K were carried forward and transferred to other aspects of corporate activities that impact several different divisions and offices. This report makes several broad recommendations to that end.

BACKGROUND

During the course of our year 2000 audit work, we reviewed all phases of the FDIC's Y2K program for both its supervisory and internal efforts using U.S. General Accounting Office (GAO) and Federal Financial Institutions Examination Council (FFIEC) guidance and other generally accepted practices to ensure that the FDIC adhered to a rigorous and structured approach to decrease its Y2K risks. We initiated our work in February 1997 by reviewing the FDIC's Y2K awareness program. We concluded that the FDIC had effectively communicated the need to address the Y2K problem, implemented an effective strategic plan, and developed needed Y2K policies and procedures for its role as a financial institution regulator and for its internal programs. Concluding that the FDIC's Y2K project appeared to be on schedule and appropriate progress was being made, we expanded the scope of our audit work to include a more comprehensive review of the FDIC's supervisory role in ensuring that the financial institutions it regulates would be Y2K compliant.

FDIC's Y2K Supervisory Efforts

In reviewing the FDIC's Y2K supervisory work, we made 37 visits to Division of Supervision (DOS) field offices and reviewed 469 Y2K assessments of financial institutions to ensure that Y2K examination results, ratings, and oversight of financial institutions were accurate, complete, and consistent. We also reviewed and provided input on the effectiveness of the Corporation's customer awareness efforts by visiting 14 banks to observe how the banks were informing their customers of the banks' Y2K readiness. We obtained literature from the banks and compared it to suggested Y2K topics developed by the FFIEC for banks communications' with consumers. We also conducted an Internet search of bank Web sites containing Y2K information and similarly analyzed this information. In total, we accessed 64 institution Web sites to perform this evaluation. We also reviewed 91 quality assurance reviews of on-site assessments covering a 5-month period -- a program that DOS adopted in response to the audit team's suggestion to provide an additional level of independent review and a method of confirming Y2K ratings. In preparing for the Y2K rollover event, we worked closely with DOS, reviewing event management plans, observing simulation exercises and Y2K tracking system tests, and providing input to DOS's event management planning and implementation efforts.

FDIC's Internal Y2K Efforts

As part of our review of the FDIC's internal program for solving the Y2K problem, we monitored the Corporation's five-phased structured program to bring all information technology, including software, hardware, telecommunications, and embedded chips into Y2K compliance. This effort included reviewing the FDIC's information technology inventories; the development of policies and procedures for testing, configuration management, and contingency planning; the FDIC's processes for assessing over 800 internal applications; the renovation and testing of those applications that were not Y2K

compliant; and the implementation of Y2K-compliant software. We also performed independent Y2K testing of selected application systems. Further, during the FDIC's preparations for the Y2K rollover, we reviewed the Division of Information Resources Management's (DIRM) action plan to ensure that it addressed all needed activities and included adequate planning for contingencies.

OIG Audit Focus and Approach

We performed our audit work in accordance with generally accepted government auditing standards. Although our audit focus was primarily on DOS and DIRM, we also reviewed other corporate Y2K efforts. We reviewed and commented on the Division of Resolutions and Receiverships' (DRR) event management planning and related simulation exercises, rollover plans for the Division of Compliance and Consumer Affairs and the Office of Corporate Communications, and corporate-wide initiatives to prepare for the Y2K rollover. During the rollover weekend, we observed and documented activities at the DOS, DRR, and DIRM communication centers, as well as the FDIC Event Management Communication Center.

We adopted a unique communication approach for this audit. We communicated process improvement opportunities to FDIC management through briefings and advisory memorandums. We provided this information as it was developed so that it would offer the greatest benefit to the Corporation. We issued nine advisory memorandums, three addressing our observations and suggestions on the FDIC's supervisory efforts, four addressing the FDIC's internal efforts, and two addressing both supervisory and internal efforts. We also summarized and provided FDIC management with best practice observations noted during our nationwide review of DOS's supervisory efforts. FDIC management responded promptly to the issues and suggestions resulting from our work.

We also prepared testimony on the status of our Y2K audit activities for the FDIC Inspector General's (IG) appearance before the Committee on Banking and Financial Services, United States House of Representatives. In that testimony, the IG explained the status of Y2K activities at the FDIC and the OIG's role in ensuring that the FDIC and financial institutions were making reasonable progress in solving the Y2K problem. We also, along with DOS and other corporate management, met with Congressional staff on two occasions to discuss the status of the FDIC's supervisory efforts.

Meeting the Challenge

Preparing for the year 2000 was a most challenging endeavor for the Corporation. The Corporation's approach was to follow the five-phase, structured approach and rigorous program management process developed by the GAO and other recognized information technology experts. The phases covered the awareness, assessment, renovation, validation, and implementation of the FDIC's Y2K program. The FDIC, in partnership with the other members of the FFIEC, developed a similar methodology to ensure that the financial institutions it supervises were prepared for the century date change.

Overall, the FDIC expended over \$105 million in personnel, hardware, software, and contracted costs through January 31, 2000 to ensure the Y2K readiness of its internal systems and operations and the financial institutions that it supervises. The OIG expended over 2,200 staff days reviewing and

providing feedback on the Corporation's activities in an effort to ensure overall Y2K success. As a result of the FDIC's commitment to this endeavor, the financial institutions generally experienced business as usual during and after the rollover, with only minor problems that were quickly corrected. In addition, the public's confidence in the banking system was maintained. On the internal side, the FDIC's investments resulted in a successful change to the year 2000 for the Corporation's information technology resources and other benefits that will extend into future operations. These benefits include accurate hardware, software, and data exchange inventories; and enhanced information technology policies and procedures that, if continued for all related DIRM operations, can improve the FDIC's overall information technology program.

RESULTS OF AUDIT

During our audit, we proactively provided management with suggestions for process improvements. On the supervisory side, we provided suggestions for (1) ensuring the consistency of Y2K assessment ratings, including issuing clarifying guidance and requiring examiners to fully develop and document assessment conclusions; (2) improving information contained in DOS's Y2K tracking system; (3) communicating Y2K assessment results in a timely manner; (4) following up with institutions to ensure that they had completed testing; (5) ensuring institutions had completed their contingency plans; and (6) implementing an independent review process for the Y2K assessment reports and related work papers.

With respect to the Corporation's internal systems, we suggested (1) updating information technology inventories to identify duplicative hardware and software, (2) improving the mission-critical application contingency planning process, (3) expanding the process used to certify applications for Y2K compliance, (4) implementing version control procedures for all computer platforms, (5) developing a business continuity and contingency plan, (6) finalizing and formalizing testing policies and procedures, and (7) correcting specific date-related issues discovered during our independent verification and validation testing.

The Corporation was successful in its efforts to transition smoothly to the year 2000, both for the financial institutions it supervises and for its internal information technology. Through its Y2K preparations, the FDIC learned many lessons that can benefit the Corporation both in future endeavors and in its daily operations. The Corporation summarized lessons learned, benefits derived, and next steps or initiatives that could be incorporated into the FDIC's normal business processes in a document entitled *Y2K – A Retrospective Look*, dated January 21, 2000. This document is an interdivisional look at the FDIC's Y2K efforts and contains our input from an audit perspective.

We believe that some practices initiated during Y2K could provide long-term benefits to the Corporation. The issues identified by our office and the Corporation that provide the greatest opportunity for continued improvements include the following:

- maintaining and periodically updating DOS's database of service providers, software vendors, and affiliated banks to facilitate solutions in the event an institution experiences problems with a servicer or vendor-supplied product;

- stressing to supervised institutions the importance of maintaining adequate business resumption and contingency plans and monitoring their maintenance of such plans;
- ensuring that internal manuals and procedures that provide operational guidance remain current;
- maintaining accurate and complete information technology inventories for the FDIC's hardware, software, and telecommunications resources;
- maintaining up-to-date and comprehensive operating procedures for FDIC buildings;
- maintaining a repository containing information on the FDIC's external data exchange partners, including points of contact, data formats, and frequencies of exchange;
- maintaining an up-to-date corporate-wide business continuity and contingency plan;
- maintaining and periodically validating the accuracy and completeness of contingency plans for mission-critical application systems;
- adopting and updating the expanded Y2K configuration management and version control program for all information technology platforms;
- incorporating the testing policies and procedures developed for Y2K into continuing FDIC policy; and
- enhancing DOS's quality assurance review program through an independent review of examination reports and supporting documentation to validate examination conclusions.

The following synopses support the benefits of sustaining the improvements listed above.

Database of Service Providers, Software Vendors, and Affiliated Banks

In preparing for potential Y2K rollover disruptions, DOS developed a database of service providers, software vendors, and affiliated banks. By doing so, DOS would be able to identify potentially affected banks in the event a service provider or software vendor experienced problems. Maintaining the completeness and accuracy of this database could aid DOS in its future supervision of financial institutions.

An additional element that could aid in the oversight of financial institutions is an inventory to track vendor-supplied application systems used by financial institutions and the versions of such applications. Information on a financial institution's use of servicers and software vendors, including which applications and versions the institution uses could be obtained during examinations and provided to a central point for use in updating the database. A periodic review of the application versions could then be performed to ensure that the financial institutions have installed any necessary application changes for their mission-critical processing.

Financial Institution Business Resumption and Contingency Plans

Prior to initiating their Y2K preparations, many financial institutions had limited contingency or disaster recovery plans. As a result of the Y2K regulatory requirements developed by the FDIC and other regulators, financial institutions developed a greater awareness of the importance of adequate business resumption and contingency plans in the event of business system disruptions. By continuing to stress the importance of maintaining, updating, and periodically testing these business resumption and contingency plans and verifying such actions by the banks, the FDIC can continue to foster an effective safeguard for both the financial institutions and the FDIC itself, as insurer.

Internal Manuals and Procedures

The FDIC's Y2K project provided the Corporation's divisions with an opportunity to review and update internal manuals and procedures, resulting in improved operational guidance. For example, during its Y2K preparations, DRR updated and reissued its closing manual. The FDIC can continue to benefit from improved operational guidance by requiring regular updates to its internal manuals and procedures.

Information Technology Inventories

As part of its Y2K program, DIRM developed and maintained inventories of information technology hardware, software, and computer applications. These inventories identified redundant, outdated, and duplicative software. Software licensing, maintenance, and operational costs can be reduced when such software is identified and eliminated. By maintaining accurate and complete IT inventories, the Corporation can more effectively manage its hardware, software and telecommunication resources.

In addition, many of the FDIC's internal applications were brought into Y2K compliance through the use of a program coding technique known as "windowing." When employing windowing, rather than physically expanding a date field to include a century date, a pivot year is used to logically identify the century. For example, if the data in a particular date field identifies the year as being between 50 and 99, 19 is logically appended to the data. If the data field identifies the year to be between 00 and 49, 20 is logically appended to the year. Although this temporary fix to the Y2K problem may continue to be effective for many years, the possibility exists that some applications may still be in service when the windowing technique is no longer effective. The FDIC can take further advantage of the current internal application inventory by adding data fields identifying the applications that employ the windowing technique and the date when the usefulness of the technique expires. By documenting this information in a single source, the FDIC will have the information needed to correctly maintain its application systems and better plan for their retirement.

Standard Operating Procedures for FDIC Buildings

To ensure the Y2K readiness of its building systems, the FDIC documented inventories of its systems and also documented standard operating procedures reflecting the operation of each building. By ensuring that the information related to each building is accurate and up-to-date, the FDIC can more

effectively manage its facilities during normal operations and in the event of unusual circumstances. Further, such actions would facilitate the transition of building operations in the event that new contractors are selected in the future.

Data Exchange Inventory

The FDIC developed a current and complete inventory of external data exchange partners during the Y2K assessment process. That process has allowed the FDIC to identify all of the external entities providing data to or receiving data from the FDIC and the associated formats of that data. This activity allowed the lines of communication between these data exchange partners to remain open and ensured that effective data exchanges occurred. The development of the data exchange inventory was a long and laborious process. Now that such an inventory has been developed, the FDIC should ensure that the information that has been collected, such as points of contact, data formats, and frequencies of exchange remain current. The information provided by the data exchange inventory will become increasingly important with anticipated increases in the use of electronic commerce throughout the public and private sectors.

Corporate Business Continuity and Contingency Plan

During our Y2K review, we suggested that the FDIC develop a Y2K business continuity plan using guidance developed by the GAO. The Chairman of the FDIC's Y2K Oversight Committee agreed and requested that our office monitor the development of a comprehensive corporate-wide business continuity plan that could serve as a basis for a Y2K-specific business continuity plan. The FDIC's development of its first comprehensive business continuity plan was labor intensive, involved all divisions and offices, and resulted in an extensive, well conceived plan to address the FDIC's critical business needs under all circumstances.

To realize continued benefits from the plan, the FDIC must ensure that the plan remains current by periodically reassessing the FDIC's business process composition; updating priorities, dependencies, and service-level requirements; reassessing failure scenarios; updating core business process risks; and defining a minimum acceptable level of core business process output. By revisiting the plan periodically, the FDIC can revalidate mission-critical business processes, prioritize these processes, and assess the risks of not meeting its stated goals. An up-to-date business continuity planning process will also assist the Corporation in developing its annual performance plan and the performance measures needed to evaluate the Corporation's success in meeting its goals and meeting the requirements of the Government Performance and Results Act of 1993 (GPRA).

Mission-Critical Application Contingency Plans

During our involvement in the Y2K process, we reviewed and commented on the Corporation's development of contingency plans to support its 35 mission-critical applications. Because in many cases the FDIC had not previously developed plans of this type, it was difficult to develop plans that adequately provided for continued operations in the event that standard processes were unavailable. Development of the plans was complex and time-consuming. However, the FDIC's efforts resulted in viable contingency plans for all of its mission-critical applications. By maintaining the plans, the FDIC will be able to respond quickly to sustain critical business operations in the event that standard processes become unavailable.

Configuration Management and Version Control Program

To control the renovation of application systems during its Y2K program, DIRM developed and issued a directive describing version control procedures for software operating on all of the FDIC's computer platforms. In addition, DIRM acquired automated tools to assist in version control activities. The ability to document and control the versions of software used in maintenance, development, and production through automated means will increase the efficiency of these operations and decrease the number of errors that can occur when moving applications from development to production. We believe that DIRM's Y2K directive was instrumental in its successful Y2K preparation by providing controls over needed application changes made to address the Y2K challenge and can continue to benefit overall DIRM software development and maintenance efforts. DIRM's directive expired on March 1, 2000. However, DIRM has established a project to develop a standard configuration management program using best practices from its Y2K experience and other sources.

Testing Policies and Procedures

DIRM expanded the FDIC's application testing policies and procedures and standardized the testing process to meet the demands of the Y2K program. These steps allowed the FDIC to systemically test the myriad of applications that were renovated during the Y2K program. Continued implementation of these expanded and standardized policies will enhance DIRM's testing of newly developed and modified application systems supporting the Corporation's mission and assist DIRM in developing performance measures to meet GPRA requirements.

Independent Review Process

During the year 2000 assessment process, DOS issued procedures that included independent field office reviews to promote consistency in examiner conclusions and to provide additional quality controls for examinations. The independent reviews were performed by individuals knowledgeable of the year 2000 assessment process and included various reporting documents, a Y2K work program, Y2K tracking system comments, and a Y2K questionnaire. DOS implemented the independent review process to address issues identified during our audit. To further validate examination conclusions, DOS implemented a quality assurance program. DOS selected statistical samples of "phase III" Y2K on-site assessments performed over a 5-month period, and senior DOS personnel, independent of the Y2K project, reviewed the related Y2K assessment documentation and concluded on the accuracy of

the Y2K ratings assigned and the effectiveness of the oversight provided.

We believe that DOS can enhance its overall supervisory program by adopting similar independent review processes to validate examiner conclusions developed during DOS's ongoing examination process.

CONCLUSIONS AND RECOMMENDATIONS

The OIG will continue to work cooperatively with corporate officials in all divisions to sustain the improvements already made so that the Corporation derives maximum benefit from its successful Y2K efforts. In that regard, we recommend overall that corporate officials continue the initiatives that worked so well during Y2K, keep the data or information related to the initiatives current, and develop the necessary policies and procedures to support and sustain the initiatives going forward. In support of these goals, we recommend that corporate officials consider the following actions:

- Maintain and keep current a database of service providers, software vendors, and affiliated banks, and add an application inventory element to the database that can be periodically reviewed to ensure that institutions have implemented important application changes. (Director, DOS)
- Advise financial institutions on the importance of periodically updating and testing their business resumption and contingency plans in the event of any possible future business disruptions and monitor institutions' actions to do so. (Director, DOS)
- Ensure that FDIC divisions and offices continually update and maintain internal manuals and procedures. (Deputy to the Chairman and Chief Operating Officer)
- Maintain current and standard information technology inventories and ensure that the internal application inventory database is expanded to include an indicator identifying application systems employing the windowing technique and the year that the usefulness of the windowing technique will expire. (Director, DIRM)
- Maintain up-to-date standard operating procedures for FDIC buildings. (Director, DOA)
- Maintain a current inventory of the FDIC's data exchange partners, including points of contact, data formats, and the frequencies of exchange. (Director, DIRM)
- Ensure that the Corporation's business continuity plan remains current. (Deputy to the Chairman and Chief Operating Officer)
- Ensure that mission-critical application contingency plans remain viable. (Director, DIRM)
- Ensure that configuration management and version control procedures adopted during the Y2K program are continued into the new millennium and are expanded to include all computer platforms. (Director, DIRM)

- Ensure that the expanded testing policies and procedures adopted for the year 2000 are continued into the new millennium. (Director, DIRM)

Additionally, with respect to the examination process itself, we recommend continuation of the initiative addressed below as providing an effective control mechanism for DOS's on-going work. This initiative reinforces recommendations and management commitments resulting from prior OIG audit work, including those contained in *DOS Actions Regarding Internet Banking* (Audit Report No. 99-043) and *Audit of Implementation of the Risk-Focused Examination Process* (Audit Report No. 98-086).

- Expand and refine DOS's independent quality assurance review program of examination reports and supporting documentation to promote consistency and to validate examination conclusions. (Director, DOS)

Because this is a special report, we did not request formal management comments. However, we met with corporate officials to discuss the contents of this report and its recommendations.

CORPORATE VIEWS

We are pleased to have received full agreement from all officials on the recommendations contained in this report. Although we did not request formal management comments, we received responses from DIRM, DOS and DOA (Attachments I, II, III respectively). The responses confirm the officials' agreement with the report contents and their commitment to continuing these initiatives going forward.

March 17, 2000

TO: Steven A. Switzer,
Deputy Inspector General

FROM: Donald C. Demitros, Director



SUBJECT: Plans for Continuing the Initiatives Identified in the OIG Draft Audit Report, "FDIC's Year 2000 Efforts"

Thank you for the opportunity to share our initiatives for transitioning best practices identified in the Y2K Project into ongoing FDIC operations. I would also like to express my appreciation for the professional support and expertise provided by the Office of the Inspector General throughout the Y2K effort. The Inspector General's contributions to this project helped to ensure the complete success of the FDIC's Y2K preparations.

In early February 2000, the Division of Information Resources Management (DIRM) Millennium IT Strategies Staff (MISS) completed a document entitled, "FDIC Year 2000 Silver Lining" which addressed lessons learned and potential process improvements for DIRM resulting from the Year 2000 Project. As evidence of the close professional relationship maintained between DIRM and the Office of the Inspector General during the Y2K Project, we have concluded that the recommendations outlined in your draft audit report are generally consistent with the recommendations generated by DIRM MISS in their Silver Linings document.

As requested in the draft audit report, the following is a brief summary of DIRM's plans for continuing the initiatives addressed in this report:

INITIATIVES HIGHLIGHTED IN THE DRAFT REPORT

- Maintain current and standard information technology inventories and ensure that the internal application inventory database is expanded to include an indicator identifying application systems employing the windowing technique and the year that the usefulness of the windowing technique will expire. (Director, DIRM)

This inventory has been uploaded to the corporate repository and is currently under the responsibility of the DIRM Data Administration Unit. With regards to the addition of an indicator identifying applications employing the windowing technique and its expiration date, based on DIRM's assessment, the only data for which the window is less than 30 is the NFC personnel data base on which one field windows around 5. As such, the overall value of

adding this indicator is extremely limited. Most of the data/applications which use windowing are vendor products, such as Microsoft office products, which are periodically updated and the technique improved or the window adjusted. Given the limited impact and risk, DIRM will not be pursuing the addition of this indicator to the inventory.

- Maintain a current inventory of the FDIC's data exchange partners, including points of contact, data formats and the frequencies of exchange. (Director, DIRM)

The inventory of FDIC data exchange partners including points of contact, data formats and frequencies of exchange is being turned over to DIRM's Data Administration Unit for ongoing maintenance within the Corporation.

- Ensure that mission critical application contingency plans remain viable. (Director, DIRM)

Maintenance of the mission critical application contingency plans is being folded into the overall FDIC Business Continuity planning effort led by DOA. DIRM will follow the schedule established under this effort to ensure timely updates and testing of these plans.

- Ensure that configuration management and version control procedures adopted during the Y2K program are continued into the new millennium and are expanded to include all computer platforms. (Director, DIRM)
- Ensure that the expanded testing policies and procedures adopted for the Y2K are continued into the new millennium. (Director, DIRM)

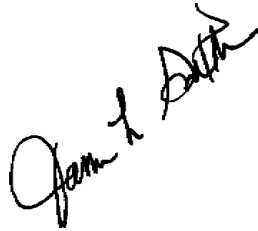
With regards to the last two recommendations, DIRM has initiated an effort, currently called "DIRM Testing, Configuration Management, and Version Control Improvement Analysis, to address the lessons learned from Y2K. This effort will continue throughout 2000 and will include detailed reviews of the DIRM testing environments, configuration management practices on all platforms, current SDLC issues related to testing and configuration management, and a variety of recent recommendations and efforts to address issues. This effort will be comprehensive with a goal of determining where process reengineering will contribute to an overall goal of delivering quality products which work the first time and are easy and inexpensive to maintain.

cc: Carol Heindel
Wayne Gooding
Martha Adams
Janet Roberson
Larry Proctor

March 23, 2000

TO: Steven A. Switzer
Deputy Inspector General

FROM: James L. Sexton
Director



SUBJECT: FDIC's Year 2000 Efforts (Audit No. 97-901)

The purpose of the memorandum is to respond to observations and recommendations delineated in your February 29, 2000 draft report relating to the FDIC's Year 2000 efforts (Audit No. 97-901). The report listed three observations and recommendations concerning work performed by the Division of Supervision (DOS). Those recommendations as well as DOS responses are presented below. They are listed in the order that they appear in the "Conclusions and Recommendations" section of your memorandum.

OIG Recommendation 1: Maintain and keep current a database of service providers, software vendors, and affiliated financial institutions, and add an application inventory element to the database that can be periodically reviewed to ensure that institutions have implemented important application changes.

DOS Response: The division currently maintains a database of service providers and financial institution with in-house computer systems in an Information Systems (IS) Examination Tracking System. Information in the database regarding service provider arrangements and/or software vendor relationships is updated at each IS examination of a financial institution or service provider.

The database presently includes a core application inventory element where specific software version and release information is maintained. IS examination procedures require that the software release number in use by a financial institution or service provider be documented at each examination. Also, examiners conclude that all vendor-released updates have been installed or determine if there are legitimate reasons why a release or update is not installed. The software version and release information is submitted with examination findings to the appropriate regional office where it is recorded in the IS Examination Tracking System.

OIG Recommendation 2: Advise financial institutions on the importance of periodically updating and testing their business resumption contingency plans in the event of any possible future business disruption and monitor institution's actions to do so.

DOS Response: A July 14, 1997 Financial Institution Letter (FIL # 68-97), entitled "FFIEC's Revised Policy Statement on Corporate Business Resumption and Contingency Planning," emphasized the importance of business recovery planning to institutions and specifically instructed institutions to ensure business resumption contingency planning and testing takes place (copy attached).

Additionally, the Division is currently working with the other FFIEC agencies to draft an interagency guidance paper discussing the lessons learned from the Year 2000 project. The guidance paper will, among other things, encourage financial institutions to conduct their own review of lessons from the Year 2000 effort and incorporate these lessons, where appropriate, in future risk management practices. One of the points addressed by the paper is the benefit of comprehensive contingency planning. DOS will ensure that the FDIC Financial Institution Letter used to distribute this interagency guidance paper reminds financial institutions of the importance of periodically updating and testing business resumption contingency plans in the event of any possible future business disruption.

DOS examiners review business resumption contingency plans and testing documentation at each IS examination. If these plans are not adequate or if periodic testing is not completed and documented, examiners cite a deficiency and recommend corrective action.

OIG Recommendation 3: Expand and refine DOS's independent quality assurance review program of examination reports and supporting documentation to promote consistency and to validate examination conclusions.

DOS Response: DOS is currently working with the Division of Research and Statistics (DRS) to enhance and refine its quality assurance program. DOS and DRS staff are working together to determine the extent of enhancement necessary. They are reviewing data such as the number of examination reports completed by each region in 1999 to determine appropriate populations for future quality assurance reviews. Independent review of a random sample of examination reports and supporting documentation will then be conducted by Internal Control and Review Section staff during Regional Office reviews and by Senior Examination Specialists or other designated Regional Office staff during Field Office reviews.

Attachment

cc: Michael J. Zamorski
John M. Lane
Simona L. Frank
Phyllis J. Zumbrun
Michael B. Benardo



Financial Institution Letters

Corporate Business Resumption and Contingency Planning

FIL-68-97
July 14, 1997

TO: CHIEF EXECUTIVE OFFICER
SUBJECT: *FFIEC's Revised Policy Statement on Corporate Business Resumption and Contingency Planning*

The interagency Federal Financial Institutions Examination Council (FFIEC) on March 26, 1997, adopted a revised policy statement on Corporate Business Resumption and Contingency Planning. The policy statement is attached.

The revised statement continues to emphasize the importance of business recovery planning and explains the goals associated with an effective business resumption and contingency plan. Revisions to the policy statement acknowledge the increased use of distributed computer environments and increased reliance on external service providers for mission-critical bank activities. A financial institution's Board of Directors is responsible for ensuring that a comprehensive business resumption and contingency plan has been implemented.

The revision was conducted as part of the combined agency Community Development and Regulatory Improvement Act (CDRIA) effort to streamline agency regulations and written policies to improve efficiency, reduce unnecessary costs, eliminate unwarranted constraints on credit availability, and remove duplicative requirements.

Contingency plans are evaluated by examiners during regular supervisory reviews of the institution. For more information, please contact your Division of Supervision Regional Office.

Nicholas J. Ketcha Jr.

Director

Attachment (below)

Distribution: FDIC-Supervised Banks (Commercial and Savings)

NOTE: Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th Street, N.W., Room 100, Washington, D.C., 20434 (202-416-6940 or 800-276-6003).

(ATTACHMENT)

CORPORATE BUSINESS RESUMPTION AND CONTINGENCY PLANNING

To: Chief Executive Officers of all Federally Supervised Financial Institutions, Senior Management of each FFIEC Agency, and all Examining Personnel

PURPOSE

This statement emphasizes to the board of Directors and senior management of each financial institution the importance of corporate business resumption and information systems contingency planning functions. This includes planning for the recovery of critical information systems processing and operations supported by external service providers. This statement also addresses issues that management should consider when developing a viable contingency plan.

BACKGROUND

Information systems technology has evolved into a critical facet of the corporate structure of financial institutions. Transaction processing and business applications are no longer restricted to mainframe computer environments. The use of distributed platforms (including mid-range computers, client/server technology, and local and wide area networks) for mission-critical business functions expands the scope of contingency planning.

Corporate and customer services throughout financial institutions are now more dependent on direct access to information and accounts. This includes contemporary financial delivery systems and services such as PC-banking, corporate cash management, and Internet promotion. These services represent key transactional, strategic, and reputational issues for the financial institutions. Often these services depend on a combination of internal and external information processing services. Outsourcing arrangements and other technology alliances involve unique considerations which also expand the boundaries of contingency planning.

Business recovery planners must recognize this new environment and the risks it may pose to the financial institution. The importance of these operations and service units requires effective business recovery planning from a corporate-wide perspective.

DEFINITION

Contingency planning is the process of identifying critical information systems and business functions and developing plans to enable those systems and functions to be resumed in the event of a disruption. The process includes testing the recovery plans to ensure they are effective. During the testing process management should also verify that business unit plans complement the information system plans.

GOALS

The goal of an effective contingency plan and recovery process is to facilitate and expedite the resumption of business after a disruption of vital information systems and operations. The principle objectives are to:

- Minimize disruptions of service to the institution and its customers.
- Ensure timely resumption of operations.
- Limit losses to earnings and capital.

It is important for both financial institutions and their service bureaus to regularly assess risks associated with the loss or extended disruption of business operations and to evaluate their vulnerability to those risks. To achieve contingency planning and business resumption goals and objectives, senior management should ensure that:

- Contingency plans are comprehensive and address all of the critical functions and operations in an institution. This includes assessing the response capability of key disaster recovery service vendors (e.g., the vendor(s) providing alternate processing sites; storage and transportation of back-up media between the storage vendor, alternate processing site and the institution).
- An effective business resumption and contingency plan has been coordinated with their information processing and service providers.¹
- Contingency plans are thoroughly tested at least annually.
- Test results and recommendations from such testing are reviewed.
- Appropriate corrective actions are implemented.

POLICY

The board of Directors and senior management of each financial institution is responsible for:

- Establishing policies and procedures, and assigning responsibilities to ensure that comprehensive corporate business resumption, contingency planning, and testing takes place.
- Annually reviewing the adequacy of the institution's business recovery and contingency plans and test results.
- Documenting such reviews and approvals in the board minutes.

Furthermore, if the financial institution receives information processing from a service bureau, senior management also has a responsibility to:

- Evaluate the adequacy of contingency planning and testing for its service bureau.
- Ensure that the institution's contingency plan is compatible with that of its service bureau.

Please refer to the FFIEC Information Systems Examination Handbook for specific guidance on developing an organization-wide contingency plan.

Revised: March 1997

¹ This concern refers to situations where service bureaus are contracted to process core applications or critical business lines. This is especially important to the Fedwire software application when the service provider is not affiliated with the institution through at least 80 percent common ownership. The institution must be able to continue its operations for these functional business lines if the service provider arrangement is terminated.

Last Updated 07/16/1999

communications@fdic.gov

[Sitemap](#) | [Search](#) | [Help](#) | [Home](#)



FDIC

Federal Deposit Insurance Corporation
550 17th Street, NW, Washington, DC 20429

CORPORATION COMMENTS

APPENDIX III

Division of Administration

March 23, 2000

MEMORANDUM TO: Steven A. Switzer
Deputy Inspector General
Office of Inspector General

FROM: Arleas Upton Kea
Director, Division of Administration

SUBJECT: Management Response to Draft Report: *FDIC's Year 2000 Efforts*

The Division of Administration (DOA) has completed its review of the draft report issued by the Office of the Inspector General (OIG) entitled *FDIC's Year 2000 Efforts*. Our review focused on those recommendations in the report addressed to the DOA. Specifically, DOA addressed two recommendations: 1) Standard operating procedures for FDIC buildings; and 2) The Corporation's business continuity plan. DOA appreciates the intensive study performed by the OIG, and the reporting of positive actions undertaken by the Corporation in addressing the technological challenges posed by the Year 2000 date change.

We agree with the conclusions of the OIG study and are in the process of or have completed the recommended changes. The report provides us with the necessary information to continue our efforts to effectively manage the FDIC's facilities.

Management Decision:

Recommendation 1: *Maintain up-to-date standard operating procedures for FDIC buildings.*

Management Response 1: We agree with the recommendation. As discussed with the OIG during a meeting with the DOA Facilities Management Section, the Standard Operating Procedures (SOPs) are current and up-to-date. DOA will continue to maintain current SOPs for FDIC buildings.

Recommendation 1: *Ensure that the Corporation's business continuity plan remains current.*

Management Response 1: We agree with the recommendation. In the fall of 1998, a Task Force was created to develop the FDIC Business Continuity Plan (Plan). In April 1999, functional responsibility was transferred to the DOA Security Management Section (SMS). In 1999, the DOA SMS engaged a Business Continuity Planning contractor to assist in better refining the overall corporate Plan. During the second half of 1999, the Corporation's efforts were fully focused on Y2K contingency planning which delayed further development of the overall Plan. Based on the lessons learned from initial testing of the Plan and the Y2K planning effort, DOA SMS is currently in the process of coordinating with each Division to re-evaluate their critical business units and core business

processes and to identify those processes that cut across divisional lines or business units. Once the critical business units and core business processes are identified, they will be integrated into a single plan structure. DOA SMS will also incorporate the communication process and notification and response procedures, developed during the Y2K planning effort, to further streamline the Plan as well as to detail the Plan's initial response and enterprise-wide communications procedures. As a result, the Plan will be more user friendly and better able to meet any business disruptions to the FDIC. DOA will also continue to periodically reassess the FDIC's business continuity plan to revalidate its mission critical business processes.

If you have any questions regarding the response, our point of contact for this matter is Andrew O. Nickle, Audit Liaison for the Division of Administration. Mr. Nickle can be reached at (202) 942-3190.

cc: Mr. Deshpande
Mr. Kmetz