United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Financial Services, House of Representatives

For Release on Delivery
Expected at 10 a.m. EST
Thursday, March 4, 2004

FEDERAL DEPOSIT INSURANCE CORPORATION

Results of 2003 and 2002 Financial Audits

Statement of Jeanette Franzel, Director
Financial Management and Assurance

GAO-04-522T

March 4, 2004

FEDERAL DEPOSIT INSURANCE CORPORATION

Results of 2003 and 2002 Financial Audits

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-522T, testimony before the Subcommittee on Oversight and Investigations, Committee on Financial Services, House of Representatives

Why GAO Did This Study

GAO is required to annually audit the financial statements of the three funds administered by the Federal Deposit Insurance Corporation (FDIC): the Bank Insurance Fund (BIF), the Savings Association Insurance Fund (SAIF), and the FSLIC (Federal Savings and Loan Insurance Corporation) Resolution Fund (FRF). GAO is responsible for obtaining reasonable assurance about whether FDIC's financial statements for BIF, SAIF, and FRF are presented fairly in all material respects, in conformity with U.S. generally accepted accounting principles, and whether FDIC maintains effective internal controls and FDIC has complied with selected laws and regulations.

Created in 1933 to insure bank deposits and promote sound banking practices, FDIC plays an important role in maintaining public confidence in the nation's financial system. In 1989, legislation to reform the federal deposit insurance system created three funds to be administered by FDIC: BIF and SAIF, which protect bank and savings deposits, and FRF, which was created to close out the business of the former Federal Savings and Loan Insurance Corporation.

GAO was asked by the Chairwoman of the House Subcommittee on Oversight and Investigations, Committee on Financial Services, to discuss the results of its February 13, 2004, report, *Financial Audit: Federal Deposit Insurance Corporation Funds' 2003 and 2002 Financial Statements* (GAO-04-429).

www.gao.gov/cgi-bin/getrpt?GAO-04-522T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Jeanette Franzel at (202) 512-9471 or franzelj@gao.gov.

What GAO Found

In reporting on the results of the 2003 and 2002 audits, GAO issued unqualified, or "clean," opinions on the three funds administered by the Federal Deposit Insurance Corporation (FDIC)—the Bank Insurance Fund (BIF), the Savings Association Insurance Fund (SAIF), and the FSLIC Resolution Fund (FRF). This means that the funds' financial statements presented fairly, in all material respects, their financial position as of December 31, 2003 and 2002. FDIC also maintained, in all material respects, effective control over financial reporting (including safeguarding of assets) and compliance with laws and regulations. GAO identified one reportable internal control weakness in the area of information system security controls, which although not considered material, is nevertheless considered a significant deficiency in the design or operation of controls.

GAO has reported weaknesses in FDIC's information systems security for a number of years. Although GAO continued to consider information security weaknesses to be a reportable condition for 2003, we also found that FDIC has made significant progress in correcting the computer security weaknesses we previously identified. FDIC took action to address current and prior-year weaknesses, including completing action on all of the 22 weaknesses that remained open from GAO's 2001 audit and 28 of the 29 weaknesses from our 2002 audit. However, GAO's work in 2003 identified 22 additional security weaknesses in FDIC's information systems. FDIC has made substantial progress in more fully implementing a computer security management program. However, it only recently established a program to test and evaluate its computer control environment and this program does not yet include all key areas. A mature, comprehensive, ongoing program of tests and evaluations of control would enable FDIC to better identify and correct information system security problems such as those found in our review.

FDIC has reported that banks and savings institutions it insures have experienced record earnings during 2003. The financial condition of BIF and SAIF are also showing positive trends. The fund balances, or net worth, for both BIF and SAIF increased during fiscal year 2003. And, the current level of estimated losses from probable failures of insured institutions is low relative to the estimated liabilities that FDIC has recorded over the last 10 years.

It is important to remember that GAO's opinions on FDIC's financial statements and its overall positive report on internal controls reflect a point in time. This also holds true for the positive financial trends that FDIC and insured financial institutions are currently experiencing. FDIC must continually monitor its business environment, assess the related risks, and adapt its internal operations as well as its insurance and supervision and monitoring functions to manage risk and maximize the value of its overall mission.

FDIC is taking action to improve its risk monitoring and operations in several areas, including financial risk management, future financial management and information needs, and information technology security and processes.

Madam Chairwoman and Members of the Subcommittee:

I am pleased to be here today to discuss the results of our audits of the Federal Deposit Insurance Corporation (FDIC) Funds' Financial Statements. We are required by the Federal Deposit Insurance Act[1] to annually audit the financial statements of the Bank Insurance Fund (BIF), the Savings Association Insurance Fund (SAIF), and the FSLIC Resolution Fund (FRF), which are administered by FDIC. Our recent report,[2] issued on February 13, 2004, presents the results of our audits of the funds' 2003 and 2002 financial statements.

Today, I will discuss the results of those audits, including the substantial progress that FDIC has made in the area of information security controls. In addition, I will provide some information on FDIC's financial condition and results and considerations for the future.

Audit Results

In our audits of the 2003 and 2002 financial statements for BIF, SAIF, and FRF, we found:

- the financial statements of each fund are presented fairly in all material respects in conformity with U.S. generally accepted accounting principles,
- although internal controls in the area of information system security should be improved, FDIC had effective internal control over financial reporting (including safeguarding of assets) and compliance with laws and regulations, and
- no reportable noncompliance with the laws and regulations we tested.

We issued unqualified or "clean" opinions on the financial statements for BIF, SAIF, and FRF. This means that the financial statements and accompanying notes for each fund presented fairly, in all material respects, the financial position as of December 31, 2003 and 2002, and the results of operations and cash flows for the years then ended and were in conformity

[1]12 U.S.C. 1827(d).

[2]*Financial Audit: Federal Deposit Insurance Corporation Funds' 2003 and 2002 Financial Statements*, GAO-04-429 (Washington, D.C.: Feb. 13, 2004).

with U.S. generally accepted accounting principles. In order to reach our conclusions about the financial statements, we (1) tested evidence supporting the amounts and disclosures in the financial statements, (2) assessed the accounting principles used and significant estimates made by management, and (3) evaluated the presentation of the financial statements. We also considered the results of our work in internal control when designing the nature and extent of our audit tests.

Regarding FDIC's internal control, we concluded that FDIC management maintained, in all material respects, effective control over financial reporting (including safeguarding of assets) and compliance as of December 31, 2003. We identified one reportable internal control weakness related to information system security controls, which although not considered material, is nevertheless considered a significant deficiency in the design or operation of controls. We also noted that FDIC made substantial progress during 2003 in this area. I will discuss FDIC's progress and the remaining work that needs to be completed in more detail in a later section of this testimony.

Our evaluation of internal control covered FDIC's financial reporting controls, which are the policies, processes, and management in place to meet the financial reporting objectives of ensuring that transactions are

- properly recorded, processed, and summarized to permit the preparation of financial statements in conformity with U.S. generally accepted accounting principles and assets are safeguarded against loss from unauthorized acquisition, use, or disposition and

- executed in accordance with laws and regulations that could have a direct and material effect on the financial statements.

In the course of performing our work on internal control, we obtained an understanding of FDIC's internal control, evaluated the design and operating effectiveness of internal control, and tested specific procedures and controls. We also considered FDIC's "control environment" and "tone at the top," which refer to management's commitment to setting and maintaining the organization's ethical tone and a positive and supportive attitude toward internal control and conscientious management.

During the course of our audit, we also tested compliance with selected provisions of laws and regulations that have a direct and material impact on the financial statements. For example, we tested for compliance with

sections of the Federal Deposit Insurance Act that require FDIC to monitor the designated reserve ratio, set semiannual assessments for each fund, and keep full and complete accounting records for all costs and expenses. Our tests for compliance with selected provisions of laws and regulations disclosed no instances of noncompliance.

This year's audit was notable in that it marked the first year that FDIC's audited financial statements were issued within 45 days of year end. FDIC's year end is December 31, and our audit report was issued on February 13, 2004. In contrast to other agencies that are making heroic efforts and using large amounts of resources to meet the accelerated reporting date, FDIC has achieved this milestone through solid financial processes and controls that help to ensure accurate and reliable financial reporting throughout the year, so that the preparation of the financial statements and the related audit can be completed in a short time after year end. We worked cooperatively with FDIC to begin accelerating the financial reporting and audit process in 2002. FDIC's accelerated reporting puts it in sync with the requirements for other federal agencies to issue their audited agency financial statements for fiscal year 2004 within 45 days of year end.[3]

FDIC Has Made Substantial Improvements in Information System Security Controls, but Weaknesses Remain

We have reported weaknesses in FDIC's information system security for a number of years. Although we continued to consider such weaknesses to be a reportable condition for 2003, we also found that FDIC has made substantial progress in correcting the security weaknesses we previously identified. FDIC took action to address current and prior-year weaknesses, including completing action on all of the 22 weaknesses that remained open from our 2001 audit,[4] and 28 of the 29 weaknesses from our 2002 audit.[5] In addition, FDIC has made substantial progress in more fully implementing an information system security management program to address the remaining weaknesses identified in our 2002 audit. Effective information system controls are essential to safeguarding financial data,

[3]Office of Management and Budget Bulletin No.01-09, *Form and Content of Agency Financial Statements* (as amended by Memorandum for Chief Financial Officers and Inspectors General dated December 21, 2001.)

[4]See U.S. General Accounting Office, *FDIC Information Security: Progress Made but Existing Weaknesses Place Data at Risk*, GAO-03-630 (Washington, D.C.: June 18, 2003).

[5]See U.S. General Accounting Office, *FDIC Information Security: Improvements Made but Weaknesses Remain*, GAO-02-689 (Washington, D.C.: July 15, 2002).

protecting computer application programs, providing for the integrity of system software, and ensuring continued operations in case of unexpected interruption.

Our work in 2003 identified 22 additional information security weaknesses in FDIC's information system. Specifically, FDIC had not adequately limited the access granted to all authorized users or completely secured access to its network. The risk created by these access weaknesses was heightened because FDIC had not completed a program to fully monitor access activity to identify and investigate unusual or suspicious access patterns that could indicate unauthorized access. Consequently, critical FDIC financial and sensitive personnel and bank examination information were at risk of unauthorized disclosure, disruption of operations, or loss of assets.

A key reason for FDIC's continuing weaknesses in information system security controls is that it has not yet fully implemented all of the elements of a comprehensive security management program. An effective program includes the following elements:

1. a central security management structure to provide overall security policy, guidance, and oversight;

2. policies and procedures that are based on risk assessments and reduction of risks to ensure that information security is addressed throughout the life cycle of each system and applicable requirements are met;

3. security awareness training to inform all users of information security risks and users' responsibilities in complying with information security policies and procedures;

4. periodic assessment of risk and magnitude of harm that could result from unauthorized access, use, or disruption of information systems; and

5. a program of testing and evaluating the effectiveness of information security policies, procedures, and practices relating to management, operational, and technical controls of every major system.

FDIC has made substantial progress in implementing a comprehensive information system security management program. Specifically, FDIC has (1) strengthened its central security management structure, (2) updated its

security policies and procedures, (3) enhanced security awareness training, and (4) developed and begun to implement a risk assessment program.

The fifth and final key element of an effective information security program is ongoing review, testing, and evaluation of information security to ensure that systems are in compliance with policies and procedures and to identify and correct weaknesses that may occur. FDIC began implementing this program during 2003. In October 2003, FDIC used a contractor to (1) develop a self-assessment process that includes annual general and application control reviews and (2) begin to perform ongoing quarterly tests of FDIC systems. While FDIC has done much to establish an ongoing program of tests and evaluations to review its computer control environment, this program does not yet address all key areas. Specifically, it does not include adequate provisions to ensure that (1) all key computer resources supporting FDIC's financial environment are routinely reviewed and tested, (2) weaknesses detected are analyzed for systemic solutions, (3) corrective actions are independently tested, and (4) newly identified weaknesses or emerging security threats are incorporated into the test and evaluation process. Incorporating these provisions into its test and evaluation process should allow FDIC to better identify and correct security problems, such as those identified in our 2003 audit.

FDIC management has shown a strong commitment to fully establishing a comprehensive security management program that includes a complete review, testing, and evaluation program. Fully establishing such a program should provide FDIC with a solid foundation for resolving computer security problems and managing its information security risks on an ongoing basis.

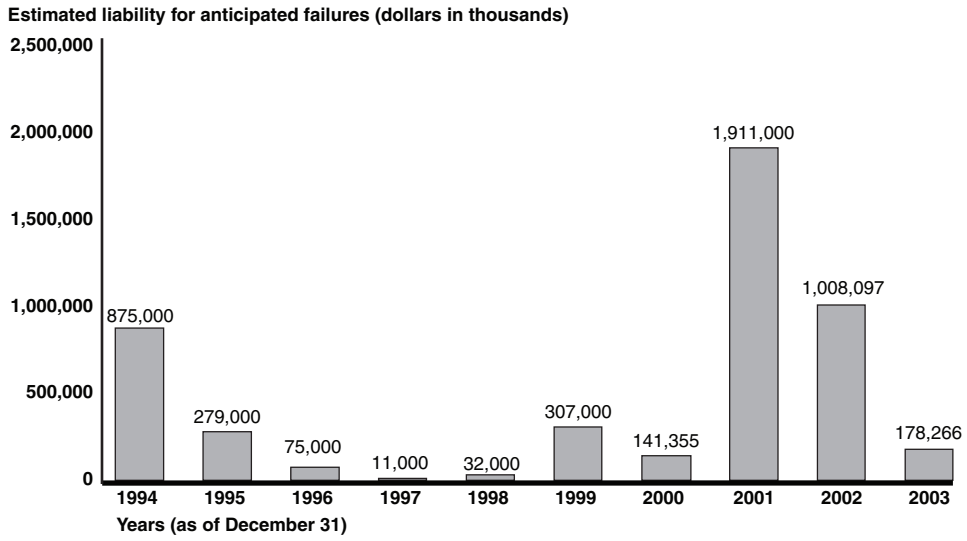
FDIC's Financial Condition and Results

The two deposit insurance funds administered by FDIC—BIF and SAIF—insured 9,182 commercial banks and savings institutions with over $9 trillion in assets and $3.5 trillion in insured deposits as of December 31, 2003. FDIC has reported that the banks and savings institutions it insures experienced record earnings during 2003. FDIC has also identified overall favorable trends in the loss provisions in the industry. However, within those trends, FDIC has noted risk and worsening asset quality in residential mortgage loans and credit cards loans.

During 2003, three BIF-insured institutions with assets of $1.1 billion failed, at an estimated cost of $103 million to the fund. At December 31, 2003, BIF had a recorded liability of $178 million in estimated losses for institutions

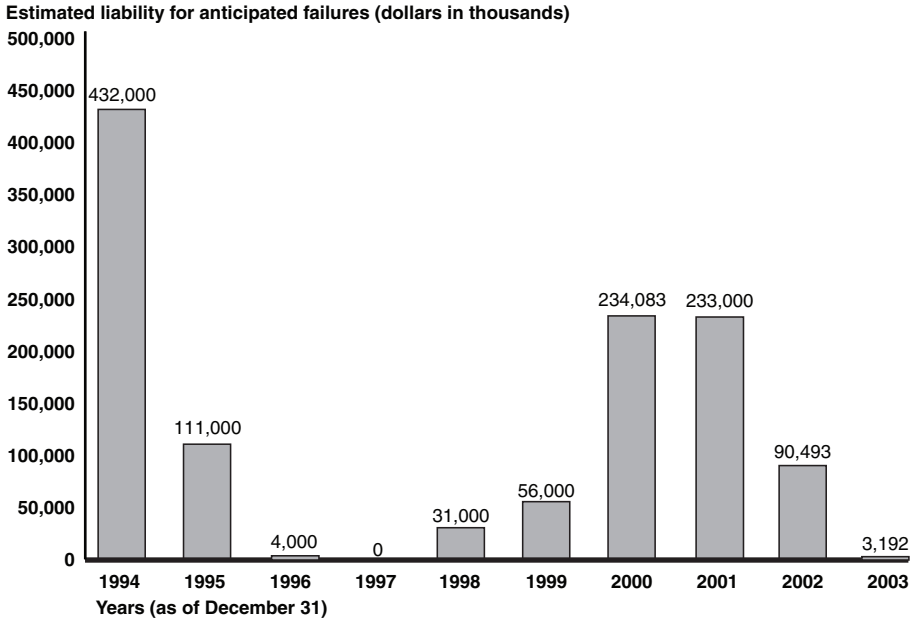
that are likely to fail within one year of the reporting date unless some favorable event occurs, such as obtaining additional capital or merging. As of December 31, 2003, SAIF had a recorded liability of $3.2 million in estimated losses for institutions that are likely to fail within one year. As shown in figures 1 and 2, the current level of estimated recorded liability for failures of insured institutions is relatively low, when compared to the estimated liabilities that FDIC recorded for probable bank failures over the past 10 years.

Figure 1: Bank Insurance Fund Estimated Liability for Anticipated Failures, December 31, 1994 through December 31, 2003



Source: BIF's audited financial statements, December 31, 1994 through December 31, 2003.

Figure 2: Savings Association Insurance Fund Estimated Liability for Anticipated Failures, December 31,1994 through December 31, 2003



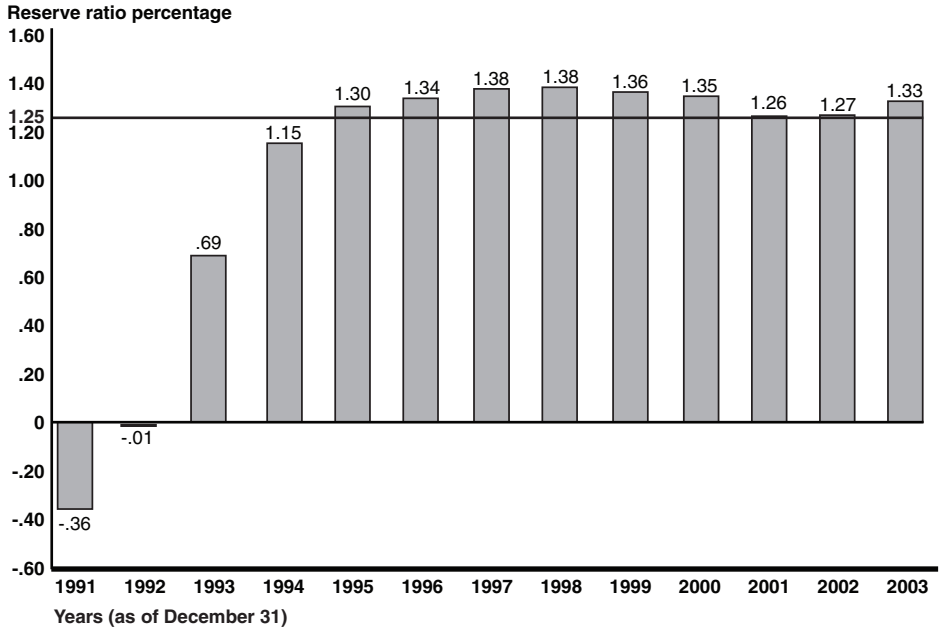
Source: SAIF's audited financial statements, December 31, 1994 through December 31, 2003.

The fund balances for both BIF and SAIF increased during fiscal year 2003. Fund balance represents the difference between assets and liabilities and is a basic measure of the funds' net worth. Fund balance also represents the cumulative net income of the funds, and each year fund balance changes by the amount of comprehensive income earned or losses incurred by the funds. As of December 31, 2003, BIF's fund balance had increased by $1.7 billion to $33.8 billion, and SAIF's fund balance had increased by $493 million to $12.2 billion. For the year ended 2003, BIF and SAIF had comprehensive income of $1.7 billion and $493 million, respectively. During 2003, assessments, interest revenue, and unrealized gains decreased from what was earned during 2002, but those decreases were more than offset in BIF and partially offset in SAIF by a reduction in the estimated losses for future failures.

The Federal Deposit Insurance Corporation Improvement Act of 1991 requires FDIC to maintain the fund balances for BIF and SAIF at a designated reserve ratio of at least 1.25 percent of estimated insured deposits. From lows significantly below 1.25 percent in 1991, the reserve

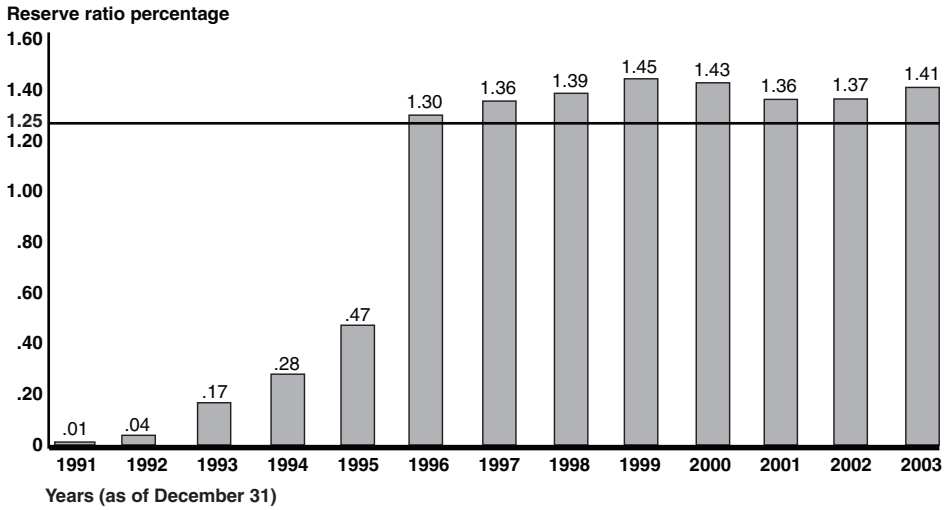
ratios of both BIF and SAIF had risen above that threshold by 1996. They have remained at or above 1.25 percent since 1996 and were at 1.33 percent for BIF and 1.41 percent for SAIF as of December 31, 2003. Figures 3 and 4 show the changes in the reserve ratio for both funds from 1991 through 2003.

Figure 3: Bank Insurance Fund Reserve Ratios from December 31, 1991 through December 31, 2003



Source: GAO calculated the reserve ratio by dividing the fund balance by the estimated insured deposits. Fund balances are from audited BIF financial statements as of December 31, 1991 through December 31, 2003. Estimated insured deposits were provided by FDIC and are unaudited.

Figure 4: Savings Association Insurance Fund Reserve Ratios from December 31, 1991 through December 31, 2003



Source: GAO calculated the reserve ratio by dividing the fund balance by the estimated insured deposits. Fund balances are from audited SAIF financial statements as of December 31, 1991 through December 31, 2003. Estimated insured deposits were provided by FDIC and are unaudited.

FDIC also manages FRF, which fulfills the obligations of the former Federal Savings and Loan Insurance Corporation and the former Resolution Trust Corporation (RTC). As of December 31, 2003, FRF had $3.5 billion in assets remaining. Of that total, $3.3 billion was in the form of cash and cash equivalents, and approximately $200 million represented estimated recoveries from receiverships for failed institutions. In contrast, FRF had $11.6 billion in assets at December 31, 1996, after it assumed the assets and liabilities of RTC. As of December 31, 2003, 52 of the 850 FRF receiverships remained active primarily due to unresolved litigation.

Considerations for the Future

It is important to remember that our opinions on FDIC's financial statements and our overall positive report on internal controls reflect a point in time. This also holds true for the positive financial trends that FDIC and insured financial institutions are currently experiencing. The banking and financial services environment is constantly changing, and in its role as insurer of financial institutions, FDIC must continually monitor its business environment, assess the related risks, and adapt its internal operations as well as its insurance and supervision and monitoring functions to manage risk and maximize the value of its overall mission.

To respond to the need to update and improve its risk monitoring and measurement process, FDIC has ongoing efforts in place to

- review and update its method for estimating the contingent liability for anticipated future failures of financial institutions;
- establish new processes to meet future financial management and financial information needs; and
- improve information technology (IT) processes, including its information system security management program.

During 2003, FDIC hired an outside consulting firm to review its financial risk management practices. The review focused on FDIC's methods and procedures for estimating the liability associated with future failures of financial institutions. FDIC initiated revisions to this methodology in the third quarter of 2003 and is planning additional revisions during 2004. FDIC last changed this methodology in 1997. The current and planned changes primarily relate to the methodology used to estimate potential failure and loss rates of insured financial institutions.

FDIC is also developing new financial systems to enhance its ability to meet future financial management and financial information needs. A related benefit of moving to more modernized systems is the ability to redirect staff resources from processing individual transactions to carrying out value-added accountability functions, such as financial analysis, decision making, and risk management functions. FDIC's current financial system was implemented in 1986, and it currently limits progress within FDIC because it is comprised of many stand-alone applications that need work-around and labor-intensive processes to interface with FDIC's core general ledger system. This current environment necessitates redundant data entry and requires the use of significant staff resources to gather and reconcile data and correct errors.

The constant changes to its operational environment require FDIC to identify opportunities to improve its computerized processes in support of operations while maintaining effective internal control and computer security. FDIC's computerized processes are key to its mission. They are critical to all of FDIC's internal operations and business lines, including insurance, supervision, consumer protection, and receivership management. With the constantly changing IT and business environment in which FDIC operates, it is critical that FDIC maintain sound IT systems,

with adequate internal control and security and applications, to effectively support and carry out its mission.

In summary, the results of our audits for 2003 were positive—clean opinions on the financial statements and overall effective internal control, with significant improvements in the area of information system security controls, which we have been reporting as a significant deficiency for several years. We have seen a strong commitment from FDIC management in promoting excellence in financial reporting and internal control. FDIC is continuing to take important steps to monitor risk, modernize its systems, and adapt to change. FDIC's mission of insuring deposits in our nation's financial institutions is critical to the citizens of this country and our nation's economy. With the banking and financial services environment constantly changing, FDIC must continually monitor its business environment and related risks, and adapt its internal operations as well as its insurance and supervision and monitoring functions to manage risk and maximize the value of its overall mission.

This testimony is based on our most recent audit of the FDIC funds' 2003 financial statements as well as our previous years' audits, which were conducted in accordance with generally accepted government auditing standards.

Madam Chairwoman, that concludes my prepared statement. I would be pleased to answer any questions you or the other members of the Subcommittee may have.

Contacts and Acknowledgments

Should you have any questions about this testimony, please contact me at (202) 512-9471 for financial issues or Robert Dacey at (202) 512-3317 for information technology issues. We can also be reached by e-mail at franzelj@gao.gov and daceyr@gao.gov. Other major contributors to this testimony were Ronald Bergman, Gary Chupka, Julia Duquette, Maxine Hattery, Dave Irvin, Meg Mills, Tim Murray, Ed Tanaka, and Charles Vrabel.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548