



United States General Accounting Office  
Washington, D.C. 20548

Comptroller General  
of the United States

To the Board of Directors  
The Federal Deposit Insurance Corporation

We have audited the balance sheets as of December 31, 2003 and 2002, for the three funds administered by the Federal Deposit Insurance Corporation (FDIC), the related statements of income and fund balance (accumulated deficit), and the statements of cash flows for the years then ended. In our audits of the Bank Insurance Fund (BIF), the Savings Association Insurance Fund (SAIF), and the FSLIC Resolution Fund (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 certain internal controls 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 that we tested.

The following sections discuss our conclusions in more detail. They also present information on (1) the scope of our audits, (2) a reportable condition<sup>1</sup> related to information system control weaknesses, and (3) our evaluation of FDIC management's comments on a draft of this report.

## Opinion on BIF's Financial Statements

The financial statements, including the accompanying notes, present fairly, in all material respects, in conformity with U.S. generally accepted accounting principles, BIF's financial position as of December 31, 2003 and 2002, and the results of its operations and its cash flows for the years then ended.

<sup>1</sup> Reportable conditions involve matters coming to the auditor's attention that in the auditor's judgment, should be communicated because they represent significant deficiencies in the design or operation of internal control and could adversely affect FDIC's ability to meet the control objectives described in this report.

---

**Opinion on SAIF's  
Financial Statements**

The financial statements, including the accompanying notes, present fairly, in all material respects, in conformity with U.S. generally accepted accounting principles, SAIF's financial position as of December 31, 2003 and 2002, and the results of its operations and its cash flows for the years then ended.

---

**Opinion on FRF's  
Financial Statements**

The financial statements, including the accompanying notes, present fairly, in all material respects, in conformity with U.S. generally accepted accounting principles, FRF's financial position as of December 31, 2003 and 2002, and the results of its operations and its cash flows for the years then ended.

---

**Opinion on Internal Control**

Although certain internal controls should be improved, FDIC management maintained, in all material respects, effective internal control over financial reporting (including safeguarding assets) and compliance as of December 31, 2003, that provided reasonable but not absolute assurance that misstatements, losses, or noncompliance material in relation to FDIC's financial statements would be prevented or detected on a timely basis. Our opinion is based on criteria established under 31 U.S.C. 3512 (c), (d) [Federal Managers' Financial Integrity Act (FMFIA)].

Our work identified weaknesses in FDIC's information system controls, which we describe as a reportable condition in a later section of this report. The reportable condition in information system controls, although not considered material, represents a significant deficiency in the design or operation of internal control that could adversely affect FDIC's ability to meet its internal control objectives. Although the weaknesses did not materially affect the 2003 financial statements, misstatements may nevertheless occur in other FDIC-reported financial information as a result of the internal control weaknesses.

---

**Compliance with Laws  
and Regulations**


Our tests for compliance with selected provisions of laws and regulations disclosed no instances of noncompliance that would be reportable under U.S. generally accepted government auditing standards. However, the objective of our audits was not to provide an opinion on overall compliance with selected laws and regulations. Accordingly, we do not express such an opinion.

---

**Objectives, Scope, and  
Methodology**

FDIC management is responsible for (1) preparing the annual financial statements in conformity with U.S. generally accepted accounting principles; (2) establishing, maintaining, and assessing internal control to provide reasonable assurance that the broad control objectives of FMFIA are met; and (3) complying with selected laws and regulations.

We are responsible for obtaining reasonable assurance about whether (1) the financial statements are presented fairly, in all material respects, in conformity with U.S. generally accepted accounting principles, and (2) management maintained effective internal control, the objectives of which are

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

We are also responsible for testing compliance with selected provisions of laws and regulations that have a direct and material effect on the financial statements.

In order to fulfill these responsibilities, we

- examined, on a test basis, evidence supporting the amounts and disclosures in the financial statements;
- assessed the accounting principles used and significant estimates made by management;
- evaluated the overall presentation of the financial statements;
- obtained an understanding of internal control related to financial reporting (including safeguarding assets) and compliance with laws and regulations;
- tested relevant internal controls over financial reporting and compliance, and evaluated the design and operating effectiveness of internal control;
- considered FDIC's process for evaluating and reporting on internal control based on criteria established by FMFIA; and
- tested compliance with selected provisions of the Federal Deposit Insurance Act, as amended, and the Chief Financial Officers Act of 1990.

We did not evaluate all internal controls relevant to operating objectives as broadly defined by FMFIA, such as those controls relevant to preparing statistical reports and ensuring efficient operations. We limited our internal control testing to controls over financial reporting and compliance. Because of inherent limitations in internal control, misstatements due to error or fraud, losses, or noncompliance may nevertheless occur and not be detected. We also caution that projecting our evaluation to future periods is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with controls may deteriorate.

We did not test compliance with all laws and regulations applicable to FDIC. We limited our tests of compliance to those deemed applicable to the financial statements for the year ended December 31, 2003. We caution that noncompliance may occur and not be detected by these tests and that such testing may not be sufficient for other purposes.

We performed our work in accordance with U.S. generally accepted government auditing standards.

FDIC management provided comments on a draft of this report. They are discussed and evaluated in a later section of this report and are reprinted in appendix I.

## Reportable Condition

In connection with the funds' financial statement audits, we reviewed FDIC's information system controls. Effective information system controls are essential to safeguarding financial data, protecting computer application programs, providing for the integrity of system software, and ensuring continued computer operations in case of unexpected interruption. These controls include the corporatwide security management program, access controls, system software, application development and change control, segregation of duties, and service continuity controls.

Although FDIC made substantial progress during the past year it has not yet fully implemented a comprehensive corporatwide security management program. An effective program includes establishing a central security function, assessing risk, establishing policies, raising user security awareness of prevailing risks, and routinely testing and evaluating the effectiveness of established controls. While FDIC has done much to establish a computer security management program, FDIC only recently established a program to test and evaluate its computer control environment, and the program did not adequately address all key areas. For example, the program did not include adequate provisions to ensure that (1) all key computer resources supporting FDIC's financial environment are routinely reviewed and tested as appropriate, (2) weaknesses detected are analyzed for systemic solutions, (3) corrective actions are independently tested, or (4) newly identified weaknesses or emerging security threats are incorporated into the test and evaluation process. A mature comprehensive ongoing program of tests and evaluations of controls would enable FDIC to better identify and correct security problems, such as those found in our review.

In our current review, we continued to identify information system control weaknesses that increased the risk of unauthorized disclosure of critical FDIC financial and sensitive personnel and bank information, disruption of critical operations, and loss of assets. Such weaknesses affected FDIC's ability to adequately ensure that users only had the access needed to perform their assigned duties and its network was sufficiently protected from unauthorized users. The risk created by these weaknesses are compounded because FDIC does not have a comprehensive monitoring program to identify unusual or suspicious access activities.

---

We determined that other management controls mitigated the effect of the information system control weaknesses on the preparation of the funds' financial statements. Because of their sensitive nature, the details surrounding these weaknesses are being reported separately to FDIC management, along with recommendations for corrective actions.

---

**FDIC Comments and Our Evaluation**

In commenting on a draft of this report, FDIC's Chief Financial Officer (CFO) was pleased to receive unqualified opinions on BIF's, SAIF's, and FRF's 2003 and 2002 financial statements. FDIC's CFO also acknowledged both the current status as well as the substantial progress made during 2003 on the information system weaknesses we identified. FDIC said it would continue efforts to strengthen its ongoing information security program during 2004.

A handwritten signature in blue ink, appearing to read "D. M. Walker", with a horizontal line extending to the right.

David M. Walker  
Comptroller General of the United States

January 30, 2004

## Appendix I



### Federal Deposit Insurance Corporation

550 17th St. NW Washington DC, 20429

Deputy to the Chairman & Chief Financial Officer

February 9, 2004

Mr. David M. Walker  
Comptroller General of the United States  
U. S. General Accounting Office  
441 G Street, NW  
Washington, DC 20548

**Re: FDIC Management Response on the  
GAO 2003 Financial Statements Audit Report**

Dear Mr. Walker:

Thank you for the opportunity to comment on the U. S. General Accounting Office's (GAO) draft audit report titled, **Financial Audit: Federal Deposit Insurance Corporation Funds' 2003 and 2002 Financial Statements**, GAO-04-429. The report presents GAO's opinions on the calendar year 2003 financial statements of the Bank Insurance Fund (BIF), the Savings Association Insurance Fund (SAIF), and the Federal Savings and Loan Insurance Corporation Resolution Fund (FRF). The report also presents GAO's opinion on the effectiveness of FDIC's internal controls as of December 31, 2003 and GAO's evaluation of FDIC's compliance with applicable laws and regulations.

We are pleased to accept GAO's unqualified opinions on the BIF, SAIF, and FRF financial statements and to note that there were no material weaknesses identified during the 2003 audits. The GAO reported that: the funds' financial statements were presented fairly and in conformity with U. S. generally accepted accounting principles; FDIC had effective internal control over financial reporting (including safeguarding of assets) and compliance with laws and regulations; and there were no instances of noncompliance with selected provisions of laws and regulations.

GAO identified the need to improve internal control over FDIC's information systems (IS) and issued a reportable condition. Although GAO identified weaknesses in FDIC's IS controls, the audit team noted that significant improvements had been made during the past year, and that the weaknesses did not materially affect the 2003 financial statements.

We acknowledge GAO's assessment of both the status and the substantial progress made in addressing the IS control environment. During 2003, FDIC's accomplishments included implementation of a recurring IS controls self assessment program, implementation of more stringent contractor personnel clearance and site security policies and procedures, and establishment of an aggressive patch management program. The FDIC will continue efforts to strengthen its ongoing, comprehensive information security program during 2004.

If you have any questions or concerns, please let me know.

Sincerely,

A handwritten signature in black ink that reads "Steven O. App".

Steven O. App  
Deputy to the Chairman and Chief Financial Officer