IV. Management Controls

As part of the Corporation's continued commitment to establish and maintain effective and efficient internal controls, FDIC management routinely conducts ongoing evaluations of internal accounting and administrative control systems. The results of these evaluations, as well as consideration of audits and reviews conducted by the U.S. General Accounting Office (GAO), the Office of Inspector General (OIG) and other outside entities, are used as a basis for the FDIC's reporting on the condition of the Corporation's internal controls.

The FDIC's management concludes that the system of internal accounting and administrative controls at the FDIC, taken as a whole, complies with internal control standards prescribed by the GAO and provides reasonable assurance that the related objectives are being met. This standard reflects the fact that all internal control systems, no matter how well designed, have inherent limitations and should not be relied upon to provide absolute assurance, and that control systems may vary over time because of changes in conditions.

The Corporation's evaluation processes, the OIG audits and the GAO financial statements audits have identified certain areas where existing internal controls should be improved. FDIC management uses the chart below in the evaluation process to determine the appropriate classification for these areas.

Effectiveness of Internal Controls

Risks	Controls are working as intended	Controls are not working as intended, but mitigating controls exist	Controls are not working as intended and minor/no mitigating controls exist
High•	OK	High Vulnerability	Material Weakness
Medium•	OK	OK	High Vulnerability or Matter for Continued Monitoring
Low•	OK	OK	Warrants Further Review

• High, Medium, and Low are measured on how potentially critical the area or operation is to achieving the mission and objectives of the Corporation. Additionally, consideration is given to the risk to the Corporation, absent the area or operation.

Material Weaknesses

For purposes of this report, FDIC management considers a weakness **material** if it:

- Violates statutory or regulatory requirements;
- Significantly weakens safeguards against waste, loss, unauthorized use or misappropriation of funds, property or other assets;
- Significantly impairs the mission of the FDIC;
- Fosters a conflict of interest;
- Deprives the public of needed services; or
- Merits the attention of the Chairman, the FDIC Board of Directors or Congress.

To determine the existence of material weaknesses, the FDIC has assessed the results of management evaluations and external audits of the Corporation's risk management and internal control systems conducted in 2002, as well as management actions taken to address issues identified in these audits and evaluations. Based on this assessment and application of the above criteria, the FDIC concludes that no material weaknesses existed within the Corporation's operations for 2002 and 2001.

High Vulnerability Issues

For purposes of this report, FDIC management has designated a high vulnerability issue as a high-risk or medium-risk area with identified deficiencies and ineffective internal controls with minor or no mitigating controls. These areas warrant special attention of management, with the need to strengthen controls. The FDIC identified Information Systems Security as a high vulnerability issue for 2002 and 2001.

Highly sensitive information is just one critical corporate resource that must be protected and managed effectively so that the FDIC can fulfill its mission. Information and analysis on banking, financial services and the economy form the basis for the development of sound public policies and promote public understanding and confidence in the nation's financial system. A strong enterprise-wide information security program is essential to the successful accomplishment of the FDIC's goals.

The FDIC has made considerable progress over the past two years in establishing a strong, effective information security program. FDIC management recognizes that this cannot be accomplished overnight but will require a continual commitment by management and the organization over a period of several years. In its report entitled *Independent Evaluation of the FDIC's Information Security Program – 2002*, the OIG concluded that "the Corporation had established and implemented management controls that provided limited assurance of adequate security of its information resources." The OIG reported that in three of ten management areas (Contractor and Outside Agency Security, Capital Planning and Investment Control, and Performance Measurement), the FDIC had no assurance that adequate security had been achieved. The FDIC is aggressively pursuing management actions in these areas.

As part of the audits of the FDIC's 2002 financial statements, GAO identified weaknesses in the FDIC's information system controls as a reportable condition. The weaknesses, although not considered material by the GAO, represented a significant deficiency in the design or operations of internal controls that could adversely affect the FDIC's ability to meet its internal control objectives. Although the GAO reported that the FDIC made progress in addressing previously identified weaknesses, the GAO stated that the lack of a fully developed and implemented comprehensive corporate-wide security management program was the primary reason for the continued weaknesses in this area. The weaknesses did not materially affect the 2002 financial statements.

In February 2002, the FDIC's Information Security Strategic Plan was approved to address these deficiencies. The plan provides for a sound information security structure and assures the integrity, confidentiality and availability of corporate information assets by proactively protecting them from unauthorized access and misuse.

During the latter part of 2002, the FDIC undertook a self-assessment of its information technology (IT) area with primary focus on information security. This self-testing was necessary to ensure that the FDIC was prepared for the 2002 GAO financial statements audit. During the self-assessment, the FDIC evaluated its progress in addressing GAO findings from earlier audits, and reviewed additional key IT areas likely to be examined by GAO during the 2002 audit. Upon completion of the self-testing, the assessment team and management recognized that

continued and immediate efforts were needed to address prior audit findings as well as newly identified high-risk areas. As a result of the self-assessment, the FDIC information security program will be considerably strengthened through more rigorous policies and procedures.

Matters for Continued Monitoring

For purposes of this report, matters for continued monitoring are medium-risk areas with ineffective internal controls with minor or no mitigating controls in place, posing medium risk to the Corporation. These areas warrant continued monitoring of corrective actions through completion.

The Pre-Exit Clearance Process was a matter for continued monitoring in the 2001 Chief Financial Officers Act (CFOA) Report. During 2002, an internal control review of the Pre-Exit Clearance Process revealed that existing controls were adequate and that access to the FDIC's systems and facilities had not been compromised by employees or contractors leaving the Corporation. As a result, this area has been removed from the continued monitoring list for the 2002 Annual Report.

The Corporation's evaluation and assessment process identified three matters that warrant continued monitoring. These matters were also included in the 2001 CFOA Report.

1 Contractor Oversight

In 2002, the FDIC continued to emphasize strong internal controls over contract oversight/project management. A number of major new systems and a significant construction project are under development and pose risk to the Corporation if not efficiently and effectively managed. Thus, it is imperative that the basic contract oversight elements of time, cost and project completion be effectively monitored and managed.

Major systems initiatives within the FDIC include the New Financial Environment (NFE), the Assessment Information Management System II (AIMS II), the Corporate Human Resources Information System (CHRIS), FDIC*connect*, FDIC XP, and Virtual Supervisory Information on the Net (ViSION). The construction project involves the building of Phase II of the Seidman Center.

NFE will provide an integrated financial system that focuses on data-sharing, state-of-the-art computing technology, and the ability to grow and change with the Corporation's future financial management and information needs. The contract is a firm fixed-price contract, and payment is based on the approval of predetermined deliverables, not on a percentage of time spent on the project. The FDIC has appointed a risk manager who is responsible for conducting an independent third-party review of NFE risks, including monitoring project cost and time, and reporting to the Chief Financial Officer and Division of Finance Director on risk-evaluation results.

AIMS II is the platform that will provide the FDIC with a flexible, robust tool to efficiently track deposit insurance assessments levied since the creation of the BIF and the SAIF in 1989, as well as any changes that pending deposit insurance reform legislation might require, including possible credits or refund calculations.

CHRIS is an integrated human resources processing and information system that will bring together the functions and data now residing in multiple stand-alone systems; it is being implemented incrementally through four versions over a four-year period.

FDIC*connect* is a secure, electronic, Web-enabled environment providing the FDIC with the capability to electronically exchange information with insured financial institutions. In 2003, the FDIC will make FDIC*connect* available to all institutions and develop several additional electronic data exchanges, including premium assessments, delivery of Financial Institution Letters, application submission and tracking information on deposit insurance.

FDIC XP is the new corporate computer software package that will provide a more stable and secure environment in which to work.

ViSION is an Internet-based data system that provides the FDIC and staff of the other federal banking agencies and state authorities access to supervisory information about financial institutions.

Phase II Construction of the Seidman Center is a project to construct a two-tower office building and multi-purpose facility at the FDIC's existing Virginia Square campus. The buildings will accommodate staff presently housed at four leased locations.

2 Risk Designation Levels/ Background Investigations

The FDIC adopted the risk designation system established by the U.S. Office of Personnel Management to provide corporate officials with a systematic, consistent and uniform way of determining risk levels of positions. The risk designation system requires FDIC officials to designate risk levels for every position in the FDIC in order to determine the type of background investigations required. In 2002, all divisions and offices were reminded to ensure that position risk designations are appropriately revised whenever the risk of a position changes. Also, the FDIC began developing a policy and procedures regarding risk designation levels and background investigations for contractors and subcontractors.

3 Business Continuity Plan

The FDIC Business Continuity Plan was developed to sustain time-sensitive operations that support mission-critical functions in the event of a disruption. While disruptions are unavoidable in some circumstances, continuity planning helps minimize negative impacts and allows the FDIC to continue meeting mission-critical requirements. In developing this plan, the FDIC considered mission goals that are central to the Corporation's operations and determined key business functions that support them.

The FDIC finalized plans for its headquarters and all regional offices. In 2002, a series of table-top exercises were conducted to test the Corporation's ability to respond to an emergency and continue critical business operations.

Internal Controls and Risk Management Program

FDIC Circular 4010.3, "FDIC Internal Control Programs and Systems," outlines steps necessary to remain in compliance with provisions of the CFOA by establishing FDIC internal control objectives, describing internal control standards, and identifying and monitoring risk management internal control programs and systems. The process focuses on areas of high risk to provide reasonable assurance that the following objectives are met:

- Programs are efficiently and effectively carried out in accordance with applicable laws and management policies;
- Assets are safeguarded against waste, loss, unauthorized use or misappropriation;
- Systems are established to alert management of potential weaknesses;
- Obligations and costs comply with applicable laws; and
- Revenues and expenditures applicable to the FDIC's operations are recorded and properly accounted for, so that accounts and reliable financial and statistical reports may be prepared and accountability of assets may be maintained.

Division and office directors are required to submit a certification statement addressed to the Chairman asserting that their internal control systems: (1) comply with the FDIC internal control standards and (2) provide reasonable assurance that the FDIC internal control objectives are achieved. The certification statement also reports whether material weaknesses, high vulnerability areas, or matters for continued monitoring exist in the internal control systems and, if so, provides a description of the deficiency and planned corrective action(s). These certification statements are used as support for the Corporation's Statements on Internal Accounting and Administrative Controls.