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 reviews of internal accounting and administrative control systems. The results of these reviews, as well as consideration of audits, evaluations 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 standards incorporate the *GAO's Standards for Internal Controls in the Federal Government*. Good internal control systems are essential for ensuring the proper conduct of FDIC business and the accomplishment of management objectives by serving as checks and balances against undesired action.

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 evaluations, 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 2003, 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 2003.

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 System Security as a high vulnerability issue for 2002 and 2003.

Adequate information system security is critical to the FDIC's accomplishment of its mission. Adequate controls are designed to provide the assurance that:

- The systems developed, enhanced and maintained provide the support necessary to carry out the objectives of the program area and provide needed information on a timely basis;
- Resources are used efficiently;
- Adequate security prevents unauthorized access to and manipulation of sensitive data;
- Data quality is preserved; and
- Operations continue in the event of a disaster.

The FDIC continues its efforts to improve the information security program and operations, but continual management attention is needed. While some challenges are amenable to near-term resolution, others can only be addressed by a concerted, continuing effort, resulting in progress over a longer period of time.

The overall assessment included in the OIG's report entitled *Independent Evaluation of the FDIC's Information Security Program – 2003* concludes that the Corporation established and implemented management controls that provided limited assurance of adequate security over its information resources. Of the ten management control areas tested, only one was rated with a control assurance level of "minimal/no assurance" in the implementation of controls category. But even in this area (Contractor and Outside Agency Security), the OIG noted that the FDIC has made significant progress since the OIG's 2002 security evaluation.

Notably, the FDIC has made considerable progress in mitigating contractor security-related risk compared to last year. Specifically, in the past year, the FDIC has updated its policy on connecting off-site contractor facilities to the corporate network and ensuring contractors are disconnected from the network when the contract expires, and has initiated a much more aggressive program to monitor and audit office activities and connections. Current plans entail inspection of contractor facilities to review security issues and concerns. By August 2003, all the sites connected to the FDIC network had been reviewed. Beginning in 2004, this approach will be expanded to include at least one scheduled and one unannounced review at each of the off-site contractor locations.

The FDIC made improvements in other areas as well. In 2002, Performance Measurement and Capital Planning/Investment Control were two areas that the OIG reported as having no assurance of adequate security. For 2003, these areas were upgraded to "limited assurance," as a result of continuous efforts made during the year. In 2003, the FDIC initiated a more extensive self-assessment program to continuously monitor and improve the Information Security Program by identifying risks and internal control deficiencies. As such, the FDIC entered into a two-year agreement with an independent contractor to assist with this initiative.

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 Corporation's evaluation and assessment process identified four matters that warrant continued monitoring. Three of these matters (numbers 2 - 4 below) were also included in the 2002 Annual Report.

1. Systems Development Project Management

The Corporation is engaged in several multi-million dollar large scale development projects, including the New Financial Environment (NFE) and the Central Data Repository (CDR). As noted by the OIG, without effective project management, the FDIC runs the risk that corporate requirements and user needs may not be met in a timely, cost-effective manner. For instance, the OIG reviewed the project control framework for the NFE and determined that a formally defined integrated framework for the project was needed. OIG felt that it would be difficult to ensure accountability and a corporate approach on the project without this integrated framework. They further determined that improvements were needed in scope management, project oversight, and time management. If corrective actions undertaken by the FDIC are not completed promptly, the project is less likely to be deployed on schedule, which may increase overall project costs.

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. Given the scope and complexity of the overall project, current delays from the original aggressive schedule, and control deficiencies identified by leadership and reinforced in the OIG's audit report number 03-045 entitled *New Financial Environment Scope Management Controls*, it is appropriate to maintain a heightened level of attention and focus on this major corporate initiative.

Also, at the FDIC's request, the OIG is reviewing issues that could impact the cost and timely completion of the CDR project. The FDIC, the Office of the Comptroller of the Currency (OCC), and the Federal Reserve Board (FRB), collectively referred to as the Federal Financial Institutions Examination Council (FFIEC) Call Agencies, want to improve the collection and management of the consolidated reports of condition and income (Call Reports) and publication of the Uniform Bank Performance Reports. This project presents potential risks and challenges as a result of the reliance on new technology and involvement of multiple agencies.

Additional audits are being planned for other large system-development efforts like Virtual Supervisory Information on the Net (ViSION). 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 IV of this project has experienced delays and potentially presents risks to timely and efficient data resource and reporting needs. Therefore, the FDIC will continue to focus heightened attention on this major initiative as well.

By continuing management focus on large scale system-development efforts, the FDIC can strengthen its internal controls and mitigate risks that could hinder the Corporation from successfully achieving its goals and objectives.

2. Contractor Oversight

Maintaining strong internal controls and effective oversight of contracting activities is critical to the FDIC's success. The Corporation's exposure to risk is greater with increased reliance on outsourcing, if those contracts are not properly managed. The FDIC is working to improve contract-management practices, including possible consolidation of the large number of existing contracts into fewer, larger, long-term contracts. This would substantially reduce the number of outstanding contractual relationships, thus allowing contract managers to focus on a more manageable number of contracts. Also, the FDIC strengthened its contract-management function by developing and implementing 25 Web-based training courses for contract oversight managers and technical monitors.

In prior years, the FDIC implemented results-oriented contracting structures for multi-year, complex high-dollar-value contracts, that linked contractor compensation with performance and greatly decreased contract administration risk. In 2003, greater emphasis (2003 Procurement Plan approved by the FDIC Board of Directors) was placed on awarding more consolidated, performance based contracting vehicles that will further enhance contractor performance and gain greater administrative efficiencies and contracting oversight.

The FDIC currently awards and administers over 50 percent of all contracting actions to support Information Technology (IT) activities within the Corporation. Other major system initiatives, in addition to NFE, CDR, and ViSION, include the Assessment Information Management System II (AIMS II), and the Corporate Human Resources Information System (CHRIS).

AIMS II is the platform that provides the FDIC with a flexible robust tool to efficiently track deposit insurance assessments levied since the creation of the BIF and SAIF in 1989. It takes into account any changes pending deposit insurance reform legislation might require, including possible credits or refund calculations. AIMS II is in production and produced the last three quarterly insurance invoices in 2003.

CHRIS is an integrated human resources processing and information system that will bring together many functions and data that now reside in multiple, stand-alone systems. CHRIS is being implemented incrementally utilizing a phased approach over a four-year period. The FDIC is currently planning the implementation of the fourth phase, which should be in production in early 2005.

A major non-systems related procurement effort now underway is the construction of Phase II of the Seidman Center (Virginia Square Phase II). This is a project that involves the addition of a two-tower office building and multi-purpose facility at the FDIC's existing Virginia Square campus. The new buildings will accommodate staff presently housed at three leased locations in Washington, DC, and will save the FDIC an estimated $78 million (in net present value terms) over a 20 year period. In September 2003, the FDIC broke ground for this new facility, which is expected to be occupied in 2006.

3. 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 the risk levels of its positions. The risk designation system requires FDIC officials to designate risk levels for every position in the Corporation to determine the type of background investigations required. In 2003, the FDIC revised its directive entitled "Security Policy and Procedures for FDIC Contractors and Subcontractors," which provides guidance and procedures for contractor risk-level designations and background investigations. The Corporation has implemented the revised requirements in this directive.

Additionally, the FDIC has revised its circular on "Personnel Suitability Program," which will give current guidance on conducting the position-based background investigations discussed above.

4. Business Continuity Plan
Business continuity planning helps to minimize the potential negative impacts of adverse developments affecting the Corporation and allows the FDIC to continue meeting mission-critical requirements. During 2003, a series of tabletop exercises and security taskforce meetings were held to evaluate current response plans and capabilities. Based on the results of these drills, response plans were revised to include lessons learned from the changing security environment.

Another related effort involved disaster recovery testing. One disaster recovery test was conducted in 2003, with several others planned for 2004 and beyond. Results of the 2003 test revealed a need to update the call listing of essential personnel and to issue new guidelines and procedures to be utilized for disaster recovery purposes.

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 Chief Financial Officers Act 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 annually, addressed to the Chairman asserting that their internal control systems: (1) comply with the FDIC's 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 issues, 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.