V. Management Controls

The FDIC's control 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 undesirable actions or outcomes.

As part of the Corporation's continued commitment to establish and maintain effective and efficient internal controls, FDIC management routinely conducts reviews of internal control systems. The results of these reviews, as well as consideration of audits, evaluations and reviews conducted by the U.S. Government Accountability 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 control activities. The FDIC's management concludes that the system of internal controls, taken as a whole, complies with internal control standards prescribed by the GAO and provides reasonable assurance that the related objectives are being met.

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. These areas are listed below.

Material Weaknesses

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 2004, as well as management actions taken to address issues identified in these audits and evaluations. Based on this assessment and application of other criteria, the FDIC concludes that no material weaknesses existed within the Corporation's operations for 2004. This is the seventh consecutive year that the FDIC has not had a material weakness.

High Vulnerability Issues

FDIC management has designated high vulnerability issues as areas requiring heightened attention of management. Although GAO did not identify a reportable condition for 2004, the FDIC identified Information Systems Security as an area of high vulnerability.

The FDIC has made significant progress in the last year to improve information systems security, but work remains to tighten and improve these controls. This assessment was confirmed by our independent auditors who reported that "FDIC made significant progress in improving its information security controls and practices; (however, these) controls provided limited assurance of adequate security over (FDIC) resources." The FDIC must ensure that processes and systems keep pace with new technologies and the growth in the types and range of attacks on systems throughout the industry.

Information system security is an inherently high-risk area due to its complexity and the existence of constant technological change. Controls need to improve to keep pace with change. Consequently, the FDIC is keeping Information Systems Security in the forefront and thus classified it as high vulnerability for 2004, despite the many accomplishments made in this area.

Matters for Continued Monitoring

FDIC management has identified four matters that warrant continued monitoring. The matters listed below are areas that are kept in the forefront of management's attention and proactively assessed throughout the year.

1. Bank Secrecy Act

The FDIC is engaged in several initiatives to strengthen its anti-money laundering (AML) supervisory program. As stated in the Management Discussion and Analysis section of this report, the Corporation has participated in interagency working groups, issued guidance and incorporated changes in examination procedures to assist in efforts to identify money laundering and terrorist financing risks. The FDIC will continue to engage in progressive initiatives, working closely with other Federal and State Regulators, FinCEN, Federal law enforcement, the Department of Homeland Security, and the State Department. A few of the initiatives include issuing comprehensive BSA/AML examination procedures; conducting nationwide industry outreach sessions focused on BSA, AML, and counter-financing of terrorism issues; increasing the number of BSA/AML subject matter experts; and providing advanced training to these subject matter experts.

2. Project Management and Contractor Oversight
The FDIC manages a variety of projects, including systems development and renovation projects. Because of the size (multi-million dollar) and complexity of some of these projects, it is imperative that the FDIC emphasize strong internal controls over project management and contractor oversight. Large, agency-wide, and complex projects pose a greater risk to the Corporation if not efficiently and effectively managed. As stated in the Message from the CFO, (pages 6-7) the FDIC's CIRC focuses on systematic review and monitoring of large-scale projects and improvements. As the FDIC is transitioning to utilizing more performance-based contracts, the Corporation is keeping a heightened level of attention on project management and contractor oversight, which is a good business practice.

3. Workforce Management
Substantial progress has been made in realigning the FDIC's workforce to reflect changes in the industry. The FDIC will be reducing staff in certain areas and increasing staff in other areas during 2005 and 2006. In addition, it will be taking the initial steps to implement the new Corporate Employee Program, which will become the foundation for a smaller, more flexible permanent workforce in the future. The Corporation will continue to monitor on an ongoing basis changes in the workload, technology, and the structure of the financial services industry and will adjust its human capital strategy, as appropriate, to address these changes.

4. Business Continuity Plan
The FDIC has developed an Emergency Preparedness Program (Program) which is comprised of an Emergency Response Plan (which addresses employee safety and security) and a Business Continuity Plan. This Corporate-wide Program continues to be refined to ensure FDIC can respond to any disruption, whether natural or man-made.

Internal Controls and Risk Management Program

Enterprise Risk Management
The FDIC is adopting an Enterprise Risk Management (ERM) approach to identifying and analyzing risks on an integrated corporate-wide basis. During 2004, the FDIC redesignated the former Office of Internal Control Management as the Office of Enterprise Risk Management. This change was intended to facilitate a shift to a more proactive and enterprise-wide approach to risk management. The focus will be on directing resources to areas of greatest risk.

The FDIC has risk managers for certain Capital Investment Review Committee (CIRC) projects. The role of these risk managers includes monitoring the schedule and budget of CIRC projects more frequently and at a more detailed level than the CIRC, interjecting risk-management concepts where needed, attending project Steering Committee meetings, and adding value as decisions are being made. Additionally, monthly risk evaluations are conducted and the results are reported to the CIRC and the Corporation's senior management.

The FDIC's circular on *FDIC Internal Control Programs and Systems* is being updated to include the concepts of ERM. The circular will provide corporate-wide guidance on risk management and internal controls from an enterprise-wide perspective. The FDIC's ERM process will continue to provide reasonable assurance that the objectives of the Federal Managers' Financial Integrity Act of 1982 (FMFIA) are met.