MANAGEMENT AND PERFORMANCE CHALLENGES

In keeping with the Reports Consolidation Act, the OIG has identified the following management and performance challenges facing the Corporation.[1] Each of the challenges we have identified is marked by one or more of the following characteristics:

1. It is important to the achievement of the FDIC mission and the strength of the nation's financial system.
2. It involves significant resources, expenditures, or fiduciary responsibility.
3. It directly impacts consumers of financial services.

The following challenges reflect the OIG's view of the Corporation's overall program and operational responsibilities; industry, economic, and technological trends; areas of congressional interest; relevant laws and regulations; the Chairman's priorities and corresponding corporate performance and Government Performance and Results Act goals; and the ongoing activities to address the issues involved.

- Assessing and Mitigating Risks to the Insurance Funds
- Ensuring Institution Safety and Soundness Through Effective Examinations, Enforcement, and Follow-Up
- Contributing to Public Confidence in Insured Depository Institutions
- Protecting and Educating Consumers and Ensuring Compliance
- Being Ready for Potential Institution Failures
- Managing and Protecting Financial, Human, Information Technology, and Procurement Resources

ASSESSING AND MITIGATING RISKS TO THE INSURANCE FUNDS

As of the end of the third quarter of 2005, the FDIC insured $3.830 trillion in deposits in 8,856 institutions. According to FDIC projections, if the current trend of industry consolidation continues, the banks the FDIC directly supervises will likely represent a smaller and smaller portion of the financial exposure it faces as deposit insurer. Also, another potential risk has become apparent as a result of recent natural disasters—multiple bank failures in a geographic region. Given these circumstances, the Corporation faces several challenges:

***Assessing Risks in Large Banks*:** To effectively fulfill its fundamental responsibilities as deposit insurer, the Corporation must ensure its large-bank program provides ready access to the information it needs to effectively identify and assess risks that large institutions, including those it does not supervise, pose to the insurance funds. Effectively communicating and coordinating with the other primary federal banking regulators is central to the Corporation's ability to meet this challenge. Moreover, given the inherent complexity of these large institutions, the FDIC must have or develop the capability to assess the risks associated with these institutions, which are different from those found in smaller banks. As the FDIC and other

[1] Under the Reports Consolidation Act, the OIG is required to identify the most significant management and performance challenges facing the Corporation and provide its assessment to the Corporation for inclusion in its annual performance and accountability report (annual report). The OIG conducts this assessment yearly and identifies a number of specific areas of challenge facing the Corporation at the time.

regulators are evaluating policy options to ensure that large institutions and the industry as a whole maintain adequate capital and reserves under Basel II, the FDIC must ensure that its staff has the necessary information and expertise to understand and evaluate the adequacy of the largest institutions' capital models. The possibility of a large bank failure, however remote, looms as a significant challenge confronting the FDIC.

***Monitoring Risks from Recent Natural Disasters*:** The FDIC and the other primary federal regulators have long emphasized the importance of disaster recovery and business continuity planning at insured depository institutions. While the focus of September 11 was on terrorist attacks and related disruption of commercial activities, recent natural disasters have added a new dimension to the risks associated with major regional crises. While initial indications from the FDIC are that the banking industry has initially fared well through the latest natural disasters, considerable risk remains over the long term to affected institutions and, in turn, the insurance funds. For example, the impact, if any, of relaxing examination and other regulatory requirements will likely not be plainly visible for many months.

***Preparing for Deposit Insurance Reform*:** The FDIC has been working with the Congress over the past several years on a comprehensive deposit insurance reform package. If enacted, the FDIC will be faced with managing the funds under the current system while transitioning under tight time constraints to a new fund structure and premium system. Implementation of operational changes may result from deposit insurance reform.

ENSURING INSTITUTION SAFETY AND SOUNDNESS THROUGH EFFECTIVE EXAMINATIONS, ENFORCEMENT, AND FOLLOW-UP

Supervision is a cornerstone of the FDIC's efforts to ensure stability and public confidence in the nation's financial system. As of September 30, 2005, the FDIC was the primary federal regulator for more than 5,250 institutions. The FDIC performs safety and soundness, Bank Secrecy Act (BSA), information technology, trust, and other types of examinations of FDIC-supervised insured depository institutions. The Corporation's system of supervisory controls must identify and effectively address financial institution activities that are unsafe, unsound, illegal, or improper before the activities cause a drain on the insurance funds. Specific challenges related to this core FDIC mission include:

***Maintaining an Effective Examination and Supervision Program*:** The FDIC has adopted a more risk-focused approach to examinations to minimize regulatory burden and better direct its resources to those areas that carry the greatest potential risk. The FDIC must continue to monitor the effectiveness of its risk-focused procedures and any related resource reductions to ensure that this approach does not compromise examination quality or results. The FDIC must also ensure that financial institutions have adequate corporate governance structures relative to the bank's size, complexity, and risk profile to prevent financial losses and maintain confidence in those entrusted with operating the institutions. The FDIC's follow-up processes must be effective to ensure institutions are promptly complying with supervisory actions that arise as a result of the FDIC's examination process.

***Supervising Industrial Loan Companies*:** The FDIC is the primary federal regulator for a number of industrial loan companies (ILCs), which are insured depository institutions owned by organizations that, as bank holding companies, are subject to a different supervisory regimen when compared to other bank holding companies. The ILC industry includes large, complex

financial institutions. The FDIC must establish and maintain effective controls in its processes for granting insurance to, supervising, and examining ILCs and their parent companies, particularly in cases where consolidated supervision is not provided by another federal regulator.

CONTRIBUTING TO PUBLIC CONFIDENCE IN INSURED DEPOSITORY INSTITUTIONS

***Guarding Against Financial Crimes in Insured Institutions*:** All financial institutions are at risk of being used to facilitate or being victimized by criminal activities including money laundering and terrorist financing. Such activities serve to undermine public confidence in the institutions. The Corporation is faced with developing and implementing programs to minimize the extent to which the institutions it supervises are involved in or victims of financial crimes and other abuse. The challenge is to facilitate the effective implementation of regulatory reporting requirements without imposing any undue regulatory burden. Examiners must also be alert to the possibility of fraudulent activity in financial institutions, which is inherently difficult because fraud is both purposeful and hard to detect.

Part of the FDIC's overall responsibility and authority to examine banks for safety and soundness is the responsibility for examining state-chartered non-member financial institutions for compliance with the Bank Secrecy Act. The BSA requires financial institutions to keep records and file reports on certain financial transactions. FDIC-supervised institutions are required to establish and maintain procedures designed to assure and monitor compliance with the BSA requirements. An institution's level of risk for potential money laundering determines the necessary scope of the BSA examination. In its role as supervisor, the FDIC also analyzes data security threats, occurrences of bank security breaches, and incidents of electronic crime that involve financial institutions. Misuse and misappropriation of personal information are emerging as major developments in financial crime. Despite generally strong controls and practices by financial institutions, methods for stealing personal data and committing fraud with that data are continuously evolving. The FDIC must continue its work in assuring the security of customer data against such criminal activity to help maintain the public's trust in the banking system.

PROTECTING AND EDUCATING CONSUMERS AND ENSURING COMPLIANCE

The FDIC protects consumers through its oversight of a variety of statutory and regulatory requirements aimed at safeguarding consumers from unfair and unscrupulous banking practices. Through community outreach efforts and technical assistance, the FDIC encourages lenders to work with members of their local communities in meeting the communities' credit needs. Specific challenges include:

***Protecting Consumer Privacy*:** The FDIC implements regulations and conducts regularly scheduled examinations to verify that institutions comply with laws designed to protect personal information, which serve to guard against the growing threat of identity theft. The FDIC evaluates the adequacy of financial institutions' programs for securing customer data and may pursue informal or formal supervisory action if it finds a deficiency.

***Educating the Public and Handling Complaints*:** The FDIC has made it a priority to impart financial education to the millions of Americans who lack basic financial skills. The

Corporation's challenge is to join with its regulatory counterparts to effectively implement programs that help integrate into the financial system the large number of households that are isolated from the opportunity to establish credit, own a home, and build a better future for their families.

Regulating Lending Practices: The FDIC's programs of supervision and education can help prevent abusive lending practices that target the financially illiterate or disadvantaged. The FDIC must evaluate laws and implement regulations to find ways to curb these lending practices, while ensuring continued access to credit for the widest range of qualified customers and protection against the abuse of vulnerable individuals. The challenge is to balance the need for regulation with avoiding inappropriate or undue interference in legitimate business activities.

Ensuring compliance with laws and regulations: The FDIC is responsible for evaluating financial institution compliance with consumer protection laws and regulations. Such laws include, for example, the Community Reinvestment Act, Home Mortgage Disclosure Act, and Fair Credit Reporting Act. In June 2003, the FDIC revised its compliance examination program. Compliance examinations now combine a risk-based examination process with an in-depth evaluation of an institution's compliance management system, resulting in a top-down, risk-focused approach to examinations. The Corporation's challenge is to ensure that the new approach makes the examination process more effective and efficient and reduces the examination burden on banks.

BEING READY FOR POTENTIAL INSTITUTION FAILURES

The FDIC is responsible for the resolution of failed banks or savings associations. The Corporation is required by law to protect taxpayers by prudently managing the Bank Insurance Fund and the Savings Association Insurance Fund and to protect insured depositors by using the assets of the funds to pay insured deposits at the time of the institution failure. The trend toward fewer failures over the past few years changes the nature of the challenge for the FDIC. Planning for failing and failed institutions, including large or multiple bank failures, needs to be evaluated, revisited, and tested for adequacy in light of FDIC downsizing activities and corresponding loss of institutional knowledge and expertise. Catastrophic events such as the multiple hurricanes that occurred during the past year underscore the need for the Corporation's readiness to respond.

MANAGING AND PROTECTING FINANCIAL, HUMAN, INFORMATION TECHNOLOGY, AND PROCUREMENT RESOURCES

The FDIC must effectively manage and utilize a number of critical strategic resources in order to carry out its mission successfully, particularly its financial, human, information technology (IT), and procurement resources. The FDIC has emphasized its stewardship responsibilities in its strategic planning process. A number of key management activities pose governance challenges to corporate executives and managers, as discussed below:

Financial Resource and Capital Investment Management: The FDIC's operating expenses are largely paid from the insurance funds, and consistent with good corporate governance principles, the Corporation must continuously seek to improve its operational efficiency.

Because 65 percent of the FDIC's budget costs are personnel-related, a challenge to the Corporation is to ensure that budgeted resources are properly aligned with workload. With respect to capital investments, effective planning and management of IT and non-IT capital investments are mandated by Congress and by the Office of Management and Budget for most federal agencies. Although many of these laws and executive orders are not legally binding on the FDIC, the Corporation recognizes that they constitute best practices and has adopted them in whole, or in part. The underlying challenge is to carry out approved investment projects on time and within budget, while realizing anticipated benefits.

Human Capital Management: In the past several years, the FDIC has undergone significant restructuring and downsizing in response to changes in the industry, technological advances, and business process improvements and, as with many government agencies, the FDIC anticipates a high level of retirement in the next 5 years. Amidst such change, the Corporation must seek to maintain employee morale and positive employee-management relationships. To that end, the FDIC formulated a human capital strategy to guide the FDIC through the rest of this decade. A key part of its human capital strategy is the Corporate Employee Program designed to help create a more adaptable permanent workforce and that reflects a more collaborative and corporate approach to meeting critical mission functions. The challenge now is implementing its strategy and monitoring the success of related human capital initiatives and programs. Additionally, developing new leaders and engaging in succession planning pose a challenge. Finally, in an age of identity theft risks, the FDIC needs to maintain effective controls to protect personal employee-related information that the Corporation possesses. The appointment of a chief privacy officer and implementation of a privacy program are positive steps toward addressing that challenge.

Information Technology Management: The FDIC seeks to maximize its IT resources to improve the efficiency and effectiveness of its operational processes. The Corporation's IT transformation initiative targets three broad areas of challenge:

- Governance and process improvements that focus on making strategic alignment a requirement for all IT work.
- Technical improvements to continue to replace/upgrade critical components of the IT infrastructure.
- Organizational changes to better align IT resources with workload, flatten the organizational structure, and improve communication with customers.

To address these broad challenges, the FDIC is embracing a capability maturity model to improve long-term business performance; employing a new system-development life cycle methodology to minimize risk, provide more predictable results, and deliver high-quality systems on time and within budget; and continuing to enhance its Enterprise Architecture (EA) program by identifying duplicative resources/investments and opportunities for internal and external collaboration to promote operational improvements and cost-effective solutions to business requirements.

The establishment of an integrated and streamlined e-government infrastructure is a key component of the Corporation's target EA. In this regard, the Corporation has initiated a number of major projects designed to improve internal operations, communications, and service to members of the public, business, and other government entities. The challenge is to ensure that such projects are consistent with e-government principles and implementing guidance from

the Office of Management and Budget, most recently guidance that is related to the use of earned value management.

Security Management—IT and Physical: The FDIC recognizes that a robust information security program requires an ongoing commitment by the organization. The OIG's 2005 Federal Information Security Management Act evaluation results showed that the Corporation had established and implemented controls in all of the management control areas assessed that provided either limited or reasonable assurance of adequate security over its information resources. Still, attention was needed in certain areas such as information security risk management, oversight of contractors with access to sensitive data and systems, and implementation of an enterprise security architecture.

Additionally, following Y2K and in light of terrorist-related disruptions and, more recently, adverse impacts of natural disasters, the importance of corporate disaster recovery and business continuity planning has been underscored and elevated to an enterprise-wide level. Such planning involves more than the recovery of the technology; it involves the recovery of the entire business. The FDIC must be sure that its Emergency Preparedness Program provides for the safety and physical security of its personnel and ensures that its critical business functions remain operational during any emergency.

Procurement Management: With corporate downsizing has come, in many instances, increased reliance on contracted services and potential increased exposure to risk if contracts are not managed properly. Processes and related controls for identifying needed goods and services, acquiring them, and monitoring contractors after the contract award must be in place and work effectively. Many employees with contracting expertise have left the Corporation and contract management responsibilities have shifted. Also, a number of new contracting vehicles and approaches are being implemented. For example, the Corporation combined approximately 40 IT-related contracts into one contract with multiple vendors for a total program value of $555 million over 10 years. Also, for the first time, it is using a large technical infrastructure contract through the General Services Administration (GSA) valued at over $300 million. Along with the expected benefits of these contracts come challenges. The Corporation has not previously outsourced a procurement process to GSA, and both new contracts are performance-based, requiring different oversight mechanisms and strategies than the time and materials contracts that the Corporation has historically used.

Enterprise Risk Management: As an integral part of its stewardship of the insurance funds, the FDIC has established a risk management and internal control program. The Corporation has committed to adopting an Enterprise Risk Management approach to identifying and analyzing risks on an integrated, corporate-wide basis. Revised OMB Circular A-123, which became effective for fiscal year 2006, requires a strengthened process for conducting management's assessment of the effectiveness of internal control over financial reporting. The circular also emphasizes the need for agencies to integrate and coordinate internal control assessments with other internal control-related activities, and ensure that an appropriate balance exists between the strength of controls and the relative risk associated with particular programs and operations.