Office of Inspector General
2007 Business Plan

The Office of Inspector General's Strategic Plan and FY 2007 Performance Plan

Also included:
FY 2007 Audit and Evaluation Plan, Planned OIG Operational Improvements, and Other Projects

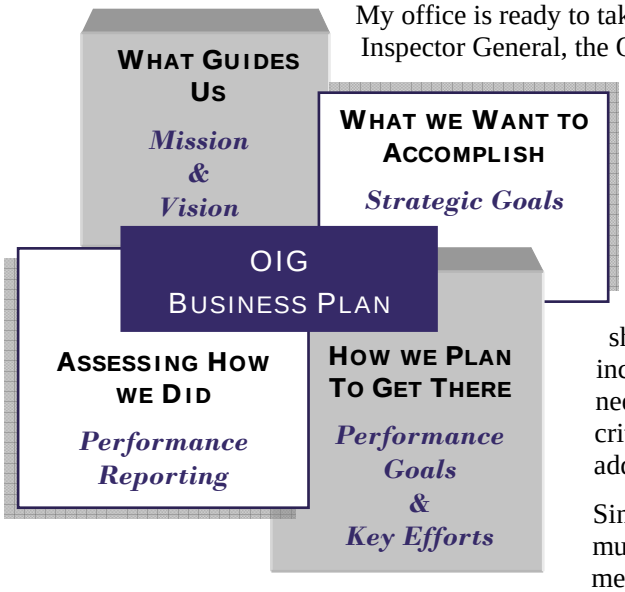
FDIC
Federal Deposit Insurance Corporation

Inspector General Foreword

November 2006

As I have shared with many over the past several months, I view our office as an integral component of the FDIC. While we are independent by statute, we are part of the FDIC team, and our job is to help the Corporation achieve its challenging mission of ensuring stability and public confidence in the nation's banking system. A recent report by the National Academy of Public Administration entitled, *Moving from Scorekeeper to Strategic Partne*r, aptly describes the role that the Office of Inspector General (OIG) can play in the federal government. Among the report's recommendations was the following:

Encourage…agency heads to maximize the use of Inspector General resources to enhance management effectiveness, efficiency, and economy. Have the Inspector General play a more proactive and constructive role in assisting agency heads in addressing management challenges.



My office is ready to take on that role. Last year under the direction of the Acting Inspector General, the OIG adopted a new business planning framework that represented concerted efforts over time to improve the OIG's planning process and sought to articulate the work of the OIG in relationship to the broader FDIC mission. In my view, establishing this framework was an important step in fostering a proactive and constructive role for the OIG. During 2006, the OIG executive team used the Business Plan to manage and assess our performance. OIG executives also held a series of outreach meetings with FDIC Division Directors that helped shape our thinking on the issues facing the FDIC, the work we have included in our Fiscal Year 2007 Business Plan, and the steps we need to take to ensure success in our office. These meetings were a critical part of our continuing efforts to ensure we are prepared to address emerging risk areas and corporate concerns.

Since becoming the Inspector General in July 2006, I have spent much time getting to know and working closely with OIG staff and meeting with the FDIC Chairman, Vice Chairman, and other corporate officials. Such dialogue has allowed me to set the future direction of our office as evidenced in this plan. Working with the OIG management team, we developed a new vision statement that will inspire us as we carry out our work: ***The OIG is a quality-focused FDIC team that promotes excellence and trust in service to the Corporation and public interest.*** Our newly formulated Office of Evaluations will play a key role in carrying out this vision.

Our 2007 plan serves as a blueprint for the audits, evaluations, investigations, and other projects in the OIG for fiscal year 2007. It also reflects our commitment to sustaining quality and increasing the efficiency of our office. To remain responsive to ever-changing priorities and emerging issues, we will keep close track of our planned work and make adjustments, as needed, to maximize the value that we add.

I am honored at the opportunity to lead the OIG and pleased to share our fiscal year 2007 plan with our stakeholders. I thank everyone for their support during my first months on the job and welcome feedback on our efforts throughout the coming year.

Jon T. Rymer [Electronically produced version; original signed by Jon T. Rymer]
Inspector General

Table of Contents

Mission, Vision, Goals, Means, and Strategies

Mission and Vision

The FDIC OIG is an independent and objective unit established under the Inspector General Act of 1978, as amended (IG Act). The OIG's mission is to promote the economy, efficiency, and effectiveness of FDIC programs and operations, and protect against fraud, waste, and abuse to assist and augment the FDIC's contribution to stability and public confidence in the nation's financial system. In carrying out its mission, the OIG conducts audits, evaluations, and investigations; reviews existing and proposed legislation and regulations; and keeps the FDIC Chairman and the Congress currently and fully informed of problems and deficiencies relating to FDIC programs and operations.

In addition to the IG Act, the OIG also has statutory responsibilities to evaluate the FDIC's information security program and practices under the provisions of the Federal Information Security Management Act of 2002, to evaluate privacy and data protection matters under Section 522 of the Consolidated Appropriations Act of 2005, and to perform material loss reviews of failed FDIC-supervised depository institutions under the provisions of the Federal Deposit Insurance Corporation Improvement Act of 1991.

Our vision is to be a quality-focused FDIC team that promotes excellence and trust in service to the Corporation and the public interest.

Strategic Goals and Performance Measures

The OIG has reviewed the FDIC operating environment looking at both long-term and short-term issues facing the Corporation. As part of the FDIC's annual reporting process, we develop "Management and Performance Challenges" reflecting significant issues that the Corporation faces in carrying out its mission. We also have met with congressional staff and monitored the issues facing the Congress in its hearings and reports, including those developed by the Government Accountability Office (GAO) in its report on "21st Century Challenges." The OIG has hosted conferences on "Emerging Issues" with participants from other OIGs of financial regulatory agencies, GAO, regulatory agency officials, and congressional staff. We also met with FDIC executives and considered the FDIC's strategic goals and the corporate priorities and objectives in developing our goals. We believe that this process has resulted in strategic goals that are mission-related and outcome-oriented, and that will contribute to the achievement of the FDIC's mission.

To help accomplish our mission and achieve our vision, the OIG has established six strategic goals. Five of these strategic goals, which are our external goals, relate to the FDIC's programs and activities. These goals are as follows:

The OIG will

- Assist the FDIC to ensure the nation's banks operate safely and soundly.
- Help the FDIC maintain the viability of the insurance fund.

- Assist the FDIC to protect consumer rights and ensure customer data security and privacy.
- Help ensure that the FDIC is ready to resolve failed banks and effectively manages receiverships.
- Promote sound governance and effective stewardship and security of human, financial, information technology, and physical resources.

In addition, we have established a sixth (internal) strategic goal:

The OIG will

- Build and sustain a high-quality OIG work environment.

Performance Measures

We are continuing the 2006 Business Plan approach to using qualitative performance measures that reflect mission-related goals and outcomes. These complement our quantitative performance measures. Each qualitative performance goal includes a set of key efforts representing ongoing work or work to be undertaken during 2007 in support of the goal. Also, potential outcomes have been identified for each performance goal to highlight the improvements that may result from these key efforts. We will measure our success in meeting our qualitative goals by having OIG senior management assess the extent to which we accomplish the work described in the key efforts under each goal. As part of our assessment, senior management will consider the amount of work conducted and recommendations made for each key effort, and then determine whether the overall body of work produced adequately achieves or addresses the related goal.

We are also continuing to use a streamlined list of quantitative measures that emphasize outcomes and results. These measures include financial benefits resulting from our audits, evaluations, and investigations; positive changes resulting from our recommendations (e.g., improved FDIC policies, practices, processes, systems, or controls); investigation actions (e.g., indictments, convictions, employee actions); recommendations implemented; and timeliness of our work products. We have revised the timeliness measures for audits, evaluations, and investigations based on our experience in FY 2006. For audits and evaluations, we will begin measuring adherence to target assignment completion dates rather than an overall average completion time. We believe this approach will permit us to better judge the extent that each assignment is meeting our timeliness goal. For investigations, we are adding a timeliness measure at the early stage of the investigation process to ensure prosecutorial interest before proceeding. Also, we are refining a timeliness measure at the end of the investigative process to ensure that we report to FDIC management on the outcome in a timely manner. A complete list of our quantitative measures, along with our targets for FY 2007, is shown in the table on page 43.

Together, our qualitative and quantitative performance measures will help us to determine the degree to which the OIG's work provides timely, quality support to the Congress, the Chairman, other FDIC officials, the banking industry, and the public. We will periodically assess the results of our performance and the appropriateness of our performance measures and goals, and make changes, as warranted.

Internal Operational Improvement Projects

This plan incorporates a number of initiatives to improve the efficiency and quality of OIG processes and products. These projects have a strategic importance for the OIG to ensure that we use our resources wisely and we can stay abreast of the significant and ever-changing challenges facing the FDIC and the banking industry.

Means and Strategies

To achieve our strategic and performance goals, we provide objective, fact-based information and analysis to the Congress, the FDIC Chairman, other FDIC officials, and the Department of Justice. This effort typically involves our audits, evaluations, or criminal investigations conducted pursuant to the IG Act and in accordance with applicable professional standards. We also make contributions to the FDIC in other ways, such as reviewing and commenting on proposed corporate policies and draft legislation and regulations; participating in joint projects with management; providing technical assistance and advice on various issues such as information technology, strategic planning, risk management, and human capital; and participating in internal FDIC conferences and seminars.

In planning and budgeting our resources, we use an enterprise-wide risk assessment and planning process that considers current and emerging industry trends, and corporate programs, operations, and risks. Our audit and evaluation assignment plan, which outlines planned audit and evaluation coverage for the coming year, is based in part on the OIG's assessment of risks to the FDIC in meeting its strategic goals and objectives. This risk-based assessment process is linked to the Corporation's program areas and the OIG's identification of management and performance challenges in those areas. In formulating our assignment plan, we solicit input from senior FDIC management and members of the FDIC Audit Committee, as well as the Congress.

Conducting investigations of activities that may harm or threaten to harm the operations or integrity of the FDIC and its programs is a key activity for achieving our goals. These investigations involve fraud at financial institutions, obstruction of FDIC examinations, misrepresentations of deposit insurance coverage, identity theft crimes, concealment of assets by FDIC debtors, or criminal or other serious misconduct on the part of FDIC employees or contractors. In conducting our investigations, we coordinate and work closely with U.S. Attorneys' Offices, other law enforcement organizations, and FDIC divisions and offices. The OIG also operates an Electronic Crimes Unit (ECU) and laboratory in Washington, D.C. The ECU is responsible for conducting computer-related investigations and providing computer forensic support to investigations nationwide. We also manage the OIG Hotline for FDIC employees, contractors, and others to report allegations of fraud, waste, abuse, and mismanagement via a toll-free number or e-mail.

Another means of ensuring we achieve our goals is to maintain positive working relationships with the Congress, the Chairman, FDIC officials, and other OIG stakeholders. We provide timely, complete, and high-quality responses to congressional inquiries and communicate regularly with the Congress about OIG work and its conclusions. Also, the OIG communicates with the Chairman and Vice Chairman through briefings about ongoing and completed work and is a regular participant at Audit Committee meetings. The OIG also places a high priority on building strong alliances with GAO, the President's Council on Integrity and Efficiency, the Executive Council on Integrity and Efficiency, and other agencies' Offices of Inspector General.

Human Capital

The OIG's employees are our most important resource for accomplishing our mission and achieving our goals. For that reason, we strive to operate a human resources program that attracts, develops, motivates, rewards, and retains a highly skilled, diverse, and capable staff.

The OIG staff is comprised of auditors, criminal investigators, attorneys, program analysts, computer specialists, and administrative personnel. The OIG staff holds numerous advanced educational degrees and possesses a number of professional licenses and certificates. To maintain professional proficiency, each of our staff attains an average of about

55 hours of continuing professional education and training annually.

Like much of the FDIC, the OIG has been downsizing its staff for several years in response to changes in the banking industry that have resulted in bank consolidations and improved financial health and the near completion of resolutions of failed institutions during the banking and thrift crises of the 1980s and early 1990s. Overall OIG staffing will have decreased from the authorized level of 190 in fiscal year 2003 to a level between 120 and 130 in fiscal year 2007. During that period, our Office of Audits has been reduced about 50 percent. These changes have impacted some performance targets compared to previous years' performance.

Information Technology

Our information technology (IT) goal is to better link IT planning and investment decisions to our mission and goals, thus helping ensure that OIG managers and staff have the IT tools and services they require to successfully and productively perform their work. The OIG IT vision is to enable our managers and staff, through reliable and modern technology, to maximize productivity and responsiveness. To help realize this goal and vision, our strategy will be to pursue IT solutions that optimize our effectiveness and efficiency, connectivity, reliability, and security, and employ best practices in managing our IT systems, services, and investments.

Relationship of the OIG to the FDIC

The IG Act, as amended, makes the OIG responsible for keeping both the FDIC Chairman and the Congress fully and currently informed about problems and deficiencies relating to FDIC programs and operations. This dual reporting responsibility makes our role unique at the FDIC and can present a number of challenges for establishing and maintaining an effective working relationship with management. Although we are an integral part of the Corporation, unlike any other FDIC division or office, our legislative underpinning requires us to operate as an independent and objective oversight unit at the same time. As such, a certain amount of tension with the Corporation may be inherent in the nature of our mission. Notwithstanding, the OIG has established a cooperative and productive relationship with the Corporation by fostering open and honest communication; building relationships based upon mutual respect; conducting our work in an objective and professional manner; and recognizing and addressing the risks, priorities, and needs of the FDIC.

FDIC Office of Inspector General
Business Plan Framework
(2007 – 2012)

Vision

The Office of Inspector General is a quality-focused FDIC team that promotes excellence and trust in service to the Corporation and the public interest.

Mission

The Office of Inspector General promotes the economy, efficiency, and effectiveness of FDIC programs and operations, and protects against fraud, waste, and abuse, to assist and augment the FDIC's contribution to stability and public confidence in the nation's financial system.

Strategic Goals

	Safety & Soundness	Insurance	Consumer Protection	Receivership Management	FDIC Resources Management	OIG Internal Processes
The OIG will	Assist the FDIC to ensure the nation's banks operate safely and soundly	Help the FDIC maintain the viability of the insurance fund	Assist the FDIC to protect consumer rights and ensure customer data security and privacy	Help ensure that the FDIC is ready to resolve failed banks and effectively manages receiverships	Promote sound governance and effective stewardship and security of human, financial, IT, and physical resources	Build and sustain a high-quality OIG work environment

FY 2007 Performance Goals

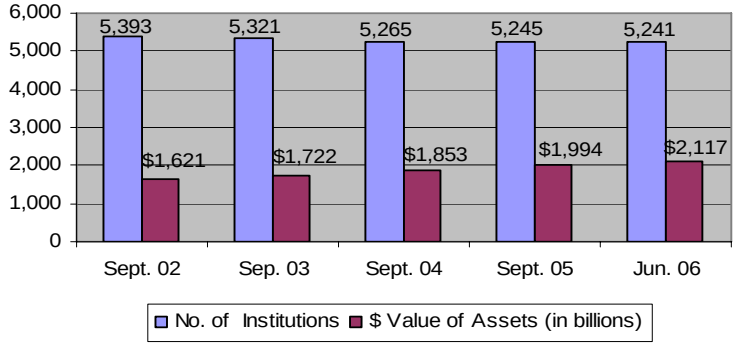
	Safety & Soundness	Insurance	Consumer Protection	Receivership Management	FDIC Resources Management	OIG Internal Processes
The OIG will	▪ Protect and ensure the effectiveness and efficiency of the FDIC's supervision program ▪ Assist FDIC efforts to detect and prevent bank secrecy act violations, money laundering, terrorist financing, fraud, and other financial crimes in FDIC-insured institutions	▪ Evaluate corporate programs to identify and manage risks that can cause losses to the fund	▪ Evaluate the effectiveness of FDIC programs for ensuring customer data security and privacy at FDIC-insured institutions ▪ Review FDIC's examination coverage of institution compliance at FDIC-supervised institutions ▪ Address allegations of fraudulent insurance coverage and identity theft schemes affecting the FDIC	▪ Evaluate the FDIC's plans and systems for managing bank resolutions ▪ Respond to potential crimes affecting FDIC's efforts to recover financial losses	▪ Evaluate corporate efforts to fund operations efficiently, effectively, and economically ▪ Assess corporate human capital strategic initiatives ▪ Promote integrity in FDIC internal operations ▪ Promote alignment of IT with the FDIC's business goals and objectives ▪ Promote IT security measures that ensure the confidentiality, integrity, and availability of corporate information ▪ Promote personnel and physical security ▪ Evaluate corporate contracting efforts ▪ Monitor corporate risk management and internal control efforts	▪ Encourage individual growth through professional development ▪ Strengthen human capital management and leadership development ▪ Foster good client, stakeholder, & staff relationships ▪ Ensure quality and efficiency of OIG audits, evaluations, investigations, and other operations ▪ Enhance strategic and annual planning & performance measurement ▪ Invest in cost-effective and secure IT

Strategic Goal 1:

The OIG Will Assist the FDIC to Ensure the Nation's Banks Operate Safely and Soundly

Bank supervision is fundamental to the FDIC's efforts to ensure stability and public confidence in the nation's financial system. As of June 30, 2006, the FDIC was the primary federal regulator for 5,241 FDIC-insured, state-chartered institutions that were not members of the Federal Reserve System (generally referred to as "state non-member" institutions). The Department of the Treasury (the Office of the Comptroller of the Currency and the Office of Thrift Supervision) or the Federal Reserve Board supervise other banks and thrifts, depending on the institution's charter. Figure 1.1 shows that while the number of institutions where the FDIC is the primary federal supervisor showed a steady decline over the past 4 years, the dollar value of assets held by those institutions showed a steady increase during the same period.

Figure 1.1: FDIC Supervised Institutions (in billions)



Source: FDIC Institution Directory

The Corporation also has back-up examination authority to protect the interests of the deposit insurance fund for more than 3,537 (as of June 30, 2006) national banks, state-chartered banks that are members of the Federal Reserve System, and savings associations.

In recent years, the banking industry has been marked by consolidation, globalization, and the development of increasingly complex investment strategies available to banks. Bank regulators, both domestically and internationally, have devised new standards for bank capital requirements commonly referred to as Basel IA and Basel II. The FDIC and the other bank regulators continue to assess the potential impact of new standards on bank safety and soundness.

The FDIC has developed and implemented programs to minimize the extent to which the institutions it supervises are involved in or victims of financial crimes and other abuse. Bank governance practices are important safeguards in this regard, and the FDIC has issued guidance to banks about governance expectations, including adherence to requirements in the Sarbanes-Oxley Act for publicly traded financial institutions. The FDIC also analyzes data security threats, occurrences of bank security breaches, and incidents of electronic crime that involve financial institutions. As part of safety and soundness examinations, the FDIC also ensures that the institutions comply with regulatory reporting requirements of the Bank Secrecy Act (BSA).

As more and more laws are passed, and new regulations are adopted to implement those laws, policy makers and regulators seek to ensure

that the intended benefits justify the considerable costs. Pursuant to the Economic Growth and Regulatory Paperwork Reduction Act of 1996, the FDIC and other bank regulators have been reviewing regulations in order to identify outdated or otherwise unnecessary regulatory requirements imposed on insured depository institutions. Notably, the President signed S.2856, the Financial Services Regulatory Relief Act. Among other provisions, this Act includes an increase from $250 million to $500 million on the asset size for eligibility for an 18-month examination cycle; permission for banks, thrifts, and credit unions to use new lending and investment authority; and other changes allowing financial institutions to improve the efficiency of their operations.

The OIG's role under this strategic goal is conducting audits and evaluations that review the effectiveness of various FDIC programs and examination processes aimed at providing continued stability to the nation's banks. Another major means of achieving this goal is through investigations of fraud at FDIC-supervised institutions; fraud by bank officers, directors, or other insiders; fraud leading to the failure of an institution; fraud impacting multiple institutions; and fraud involving monetary losses that could significantly impact the institution.

2007 Performance Goals: To assist the FDIC to ensure the nation's banks operate safely and soundly, the OIG will

- Protect and ensure the effectiveness and efficiency of the FDIC's Supervision Program, and
- Assist FDIC efforts to detect and prevent BSA violations, money laundering, terrorist financing, fraud, and other financial crimes in FDIC-insured institutions.

2007 Performance Goal 1.1:

Protect and ensure the effectiveness and efficiency of the FDIC's supervision program.

Key Efforts

- Be prepared to conduct material loss reviews and report on failures of FDIC-supervised insured depository institutions, as mandated. As part of such preparation, explore the development of a virtual material loss review with the Corporation. **[AUDIT]**
- Determine whether the FDIC's examinations comply with applicable policies and procedures for addressing an institution's sensitivity to interest rate changes and evaluate how examiners consider off-site and industry-wide analysis in assessing interest rate risk. **[AUDIT]**
- Determine whether the FDIC's examination procedures address the risks associated with electronic banking and the extent to which examiners follow those procedures. **[AUDIT]**
- Assess the FDIC's oversight of subprime lending at FDIC-supervised institutions, including examination guidance, policy, and related training. **[AUDIT]**
- Determine whether FDIC IT examinations comply with Federal Financial Institutions Examination Council examination processes for technology service providers (TSPs) at independent data centers. **[AUDIT]**
- Determine whether the FDIC's examinations adequately consider the reliability of appraisals and sufficiency of insurance coverage when evaluating an institution's lending activities. **[AUDIT]**

Significance

The Federal Deposit Insurance (FDI) Act, requires the cognizant OIG to perform a review when the deposit insurance fund incurs a material loss due to the failure of an insured depository institution. The FDIC OIG performs the review if the FDIC is the primary regulator of the institution. The Department of the Treasury OIG and the OIG at the Board of Governors of the Federal Reserve System perform reviews when their agencies are the primary regulators. These reviews identify what caused the material loss, evaluate the supervision of the federal regulatory agency (including compliance with the Prompt Corrective Action requirements of the Federal Deposit Insurance Act), and propose recommendations to prevent future failures. A loss is considered material to the insurance fund if it will exceed $25 million and 2 percent of the failed institution's total assets. While no banks or thrifts have failed in the United States since June 25, 2004, the OIG must be prepared to conduct such a review, as necessary, and will work with the Division of Supervision and Consumer Protection (DSC) and the Division of Resolutions and Receiverships (DRR) to ensure such readiness.

The examination of the banks that it regulates is a core FDIC function. Through this process, the FDIC assesses the adequacy of management and internal control systems to identify, measure, and control risks; and bank examiners judge the safety and soundness of a bank's operations. The Corporation conducted 2,399 safety and soundness examinations in 2005. The examination program employs risk-focused supervision for banks. According to examination policy, the objective of a risk-focused examination is to effectively evaluate the safety and soundness of the bank, including the assessment of risk management systems, financial condition, and compliance with applicable laws and regulations, while focusing resources on the bank's highest risks.

The OIG's work in 2007 will focus on how effective the FDIC's examinations are in assessing a variety of risks that can be particularly sensitive for banks. In one audit, we will focus on an assessment of interest rate risks. In another audit, we will review added risks associated with electronic banking, and determine whether examination procedures adequately address the risks and the extent to which the examiners follow the procedures. Another assignment will address examination coverage of an institution's lending activities with attention to the reliability of appraisals and sufficiency of insurance coverage.

Similarly, with respect to subprime lending, since the 1990's, such lending volumes have increased significantly and financial regulators have closely monitored and responded to that trend. However, any weaknesses in the related examination guidance and the FDIC's implementation of that guidance may impact an institution's safety and soundness.

Finally, banks often outsource software development and maintenance, data processing, and other critical IT business services to TSPs. Many of these services fall within the purview of bank examiners, and for FDIC-supervised institutions, it is through IT examinations that the coverage occurs. One of the OIG's audits in 2007 will determine whether the FDIC's examinations of TSPs comply with applicable guidance. Given the industry's widespread use of TSPs, any financial or operational problems that TSPs experience could negatively impact the safety and soundness of multiple institutions.

Potential Outcomes

- Effective, efficient readiness of staff for Material Loss Review work.
- Improved bank supervision to identify and correct unsafe and unsound banking practices.
- Assurance that banks appropriately manage their interest rate risks.
- Enhanced protection from risks associated with electronic banking.
- Enhanced protection from risks associated with subprime lending.
- Assurance that IT examinations provide appropriate coverage of TSPs.

2007 Performance Goal 1.2:

Assist FDIC efforts to detect and prevent bank secrecy act violations, money laundering, terrorist financing, fraud, and other financial crimes in FDIC-insured institutions.

Key Efforts

- Conduct investigations based on allegations of fraud at open FDIC-supervised institutions and closed institutions, including investigations involving attempts to obstruct examinations. **[INVESTIGATION]**
- Collaborate with DSC and the Legal Division to maximize mutual benefits to be derived from parallel criminal/civil enforcement proceedings. **[INVESTIGATION]**
- Participate in Regional DSC/Legal review committees to identify at the earliest possible stage, those financial institution fraud cases of greatest significance to the FDIC. **[INVESTIGATION]**
- Participate in interagency working groups addressing fraud affecting financial institutions. **[INVESTIGATION]**
- Develop industry outreach initiatives to inform financial institutions and the banking community on fraud-related issues and the role of the OIG in deterring and combating such fraud. **[OTHER PROJECT]**
- Operate a Suspicious Activity Report (SAR) database to enhance the OIG Office of Investigations (OI) and DSC's ability to identify, analyze, and address fraud cases impacting the FDIC and participate in other law enforcement/regulatory task groups formed to review the SARs. **[OTHER PROJECT]**
- Determine whether examination procedures are designed to effectively evaluate institution compliance with the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) anti-money laundering and terrorist financing provisions and examiners are fully and consistently implementing the procedures. **[AUDIT]**
- Determine whether DSC provides effective supervision of FDIC-supervised institutions' compliance with Office of Foreign Assets Control requirements. **[AUDIT]**

Significance

All financial institutions today are at risk of being used to facilitate criminal activities, including money laundering and terrorist financing. The Corporation needs to guard against a number of

financial crimes and other threats, including money-laundering, terrorist financing, data security breaches, and financial institution fraud. Bank management is the first line of defense against fraud, and the banks' independent auditors are the second line of defense. Because fraud is both purposeful and hard to detect, it can significantly raise the cost of a bank failure, and examiners must be alert to the possibility of fraudulent activity in financial institutions.

The OIG's OI works closely with FDIC management in DSC and the Legal Division to identify and investigate financial institution crime, especially fraud. OIG investigative efforts are concentrated on those cases of most significance or potential impact to the FDIC and its programs. The goal, in part, is to bring a halt to the fraudulent conduct under investigation, protect the FDIC and other victims from further harm, and assist the FDIC in recovery of its losses. Pursuing appropriate criminal penalties not only serves to punish the offender but can also deter others from participating in similar crimes.

Since the terrorist attacks of September 11, 2001, the FBI has no longer been able to devote the same level of resources to financial institution fraud cases. The OIG fully expects its caseload of financial institution fraud to continue to increase. U.S. Attorneys' Offices and FBI Offices throughout the country are increasingly relying on the FDIC OIG to handle such cases. Referrals and requests for investigative assistance from the U.S. Attorneys' Offices and the FBI are on the increase. The OIG is also receiving more referrals of financial institution fraud matters from DSC. We expect such referrals to continue to increase, particularly because our criminal investigations can also be of benefit to the FDIC in pursuing enforcement actions to prohibit offenders from continued participation in the banking system.

The intentional denial of accurate information to bank examiners undermines the integrity of the examination process. When investigating instances of financial institution fraud, the OIG defends the vitality of the FDIC's examination program by investigating associated allegations or instances of criminal obstruction of bank examinations and by working with U.S. Attorneys' Offices to bring these cases to justice.

The OIG's investigations of financial institution fraud currently constitute about 75 percent of the OIG's investigation caseload. At year-end 2001, the OIG had 43 open financial institution fraud cases. That number had risen to 97 by year-end 2006.

The OIG is also committed to continuing its involvement in interagency forums addressing fraud. Such groups include national and regional bank fraud, check fraud, mortgage fraud, cyberfraud, identity theft, and anti-phishing working groups. Additionally, the OIG will enhance its industry outreach efforts to keep financial institutions informed on fraud-related issues and to educate bankers on the role of the OIG in combating financial institution fraud.

A number of significant laws drive the OIG's work with respect to this strategic goal. Under the BSA, banks must file a Currency Transaction Report (CTR) with the Treasury Department for each transaction over $10,000 or multiple cash transactions by any individual in one business day or over the period of a day aggregating over $10,000. The BSA also requires banks to file SARs when suspected money laundering or BSA violations occur. Although the Department of the Treasury has overall authority for BSA enforcement and compliance, the Financial Crimes Enforcement Network (FinCEN), created in 1990, has delegated authority to administer the BSA. FinCEN maintains automated systems from which DSC examiners can download information on CTRs and SARs filed by FDIC-supervised institutions. The filing and use of SARs and CTRs has been the subject of significant regulatory, congressional, and banking community interest. Our efforts to establish a data base of SARs will augment our capability to search and sort data from FinCEN and assist OIG investigations and DSC enforcement actions.

The USA PATRIOT Act, enacted on October 26, 2001 in response to the September 11, 2001 terrorist attacks, made a number of amendments to the anti-money laundering provisions of the BSA. Title III of the USA PATRIOT Act, in particular, is intended to facilitate the prevention, detection, and prosecution of international money laundering and terrorist financing. FDIC examiners play a critical role in ensuring that institutions comply with the Act, and we will be reviewing this area in 2007. Examiners must consistently implement procedures to help ensure that institutions have needed programs in place to detect money laundering and terrorist financing activities that can threaten the safety and soundness of institutions and the security of American citizens.

In a related vein, the Department of the Treasury's Office of Foreign Assets Control (OFAC) is responsible for developing, promulgating, and administering sanctions for the Secretary of the Treasury under various laws, including the Trading with the Enemy Act and the International Emergency Economic Powers Act. Generally, OFAC regulations prohibit financial institutions from engaging in transactions with the governments of, or individuals or entities associated with, foreign countries against which federal law imposes economic sanctions. As referenced earlier, the FDIC's safety and soundness examinations of FDIC-supervised financial institutions include an assessment of the institutions' compliance with BSA anti-money laundering requirements. As part of the BSA anti-money laundering examinations, the FDIC assesses the institution's OFAC compliance programs. The OIG's work will look at the FDIC's efforts in this area.

Potential Outcomes

- Reduced opportunity for fraud to take place within financial institutions.
- FDIC recovery of losses from financial institution fraud and avoidance of further harm.
- Assessment of criminal and civil penalties, where appropriate, and deterrence of others from participating in similar crimes.
- Improved financial institution measures to prevent, detect, and pursue potential money laundering and terrorism financing activity.
- Enhanced OIG and DSC use of SARs to pursue potential money laundering and terrorist financing cases and activities.
- Increased assurance that the U.S. financial system is not used for illicit purposes.
- Information/best-practice sharing with industry representatives, broader understanding of risks of fraud occurring in institutions, and heightened understanding of the role of the OIG in combating fraud.

Strategic Goal 2:

The OIG Will Help the FDIC Maintain the Viability of the Insurance Fund

Federal deposit insurance remains a fundamental part of the FDIC's commitment to maintain stability and public confidence in the Nation's financial system. Now in its eighth decade, the FDIC has insured deposits up to the legally authorized threshold, which presently stands at $100,000 for individual accounts and $250,000 for retirement accounts. Legislation passed by the Congress on February 1, 2006 merges separate insurance funds for banks and thrifts into a single Deposit Insurance Fund with about $50 billion in reserve. This legislation also imposed some reforms on how the FDIC is to manage the fund in the future including indexing for inflation, permitting the fund reserves to fluctuate inside a percentage range of estimated insured deposits, and administering rebates and assessments. The Corporation is working to implement these reforms.

As insurer, the FDIC must also evaluate and effectively manage how changes in the economy, the financial markets, and the banking system affect the adequacy and the viability of the Deposit Insurance Fund. Significantly, there has been no bank or thrift failure in over 2 years for the first time in the FDIC's history. Still, there remain many challenges to the FDIC and other banking regulators.

The continuing consolidation of the banking industry means there are a few very large institutions that represent an increasingly significant share of the Deposit Insurance Fund's risk exposure. Industry consolidation presents benefits and risks to the Deposit Insurance Fund. While the risks to the funds are diminished because of the diversification benefits of consolidation (along geographic and product lines), the concentration of deposits in fewer insured depository institutions increases the risks to the Deposit Insurance Fund in the event a large insured depository institution fails.

As a result of industry consolidation, the assets in the industry are also increasingly concentrated in a small number of large, complex institutions for which the FDIC is not, for the most part, the primary supervisor. The largest banks operate highly complex branch networks, have extensive international and capital market operations, and work on the cutting edge of technologically sophisticated finance and business. The increased complexity of the industry and the concentration of risk to the insurance funds in the largest banking organizations are expected to grow more pronounced over time and to present greater risk-management challenges to the Corporation. A two-tiered banking system characterized by a limited number of very large, complex institutions and a much larger number of small community banks appears to be emerging. The banking regulators, including the FDIC, need insight into the risks that are inherent in these different types of banking organizations.

The OIG has a responsibility to evaluate the FDIC's programs and operations to ensure that the agency has adequate information to gauge the risks inherent as financial institutions consolidate, enter into new business areas, and become more global.

2007 Performance Goals: To help the FDIC maintain the viability of the deposit insurance fund, the OIG will

- Evaluate corporate programs to identify and manage risks in the banking industry that can cause losses to the fund.

2007 Performance Goal 2.1:

Evaluate corporate programs to identify and manage risks that can cause losses to the fund.

Key Effort

- Evaluate FDIC's External Risk Management Approach. **[EVALUATION]**
- Review the Dedicated Examiner Program. **[AUDIT]**

Significance

The FDIC, in cooperation with the other primary federal regulators, proactively identifies and evaluates the risk and financial condition of every insured depository institution. The FDIC also identifies broader economic and financial risk factors that affect all insured institutions. The availability of timely banking information is critical to ensuring the FDIC's ability to assess risk to insured financial institutions and the deposit insurance funds. The FDIC is committed to providing accurate and timely bank data related to the financial condition of the banking industry. Industry-wide trends and risks are communicated to the financial industry, its supervisors, and policymakers through a variety of regularly produced publications and ad hoc reports. Risk-management activities include approving the entry of new institutions into the deposit insurance system, off-site risk analysis, assessment of risk-based premiums, and special insurance examinations and enforcement actions.

Risk management begins with the FDIC's review of applications for deposit insurance to ensure that the applying institution is well-capitalized, possesses a qualified management team, and is capable of operating in a safe and sound manner.

Off-site risk analysis activities include reviewing examination reports and using a variety of information system models and tools. The purposes of these activities are to understand the risk profile of individual financial institutions and to identify trends and emerging risks affecting groups of financial institutions and the insurance fund. The information may be used to target institutions for examination or other follow-up activities; focus the scope of an examination; assist in setting risk-based premiums for individual institutions; determine the adequacy of the deposit insurance fund; develop new policy initiatives; and determine corporate strategies for supervision, staffing, communication and other resource decisions.

Primary responsibility for identifying and managing risks to the Deposit Insurance Fund lies with the FDIC's Division of Insurance and Research, DSC, and DRR. To help integrate the risk management process, the FDIC established the National Risk Committee (NRC), a cross-divisional body. Also, a Risk Analysis Center monitors emerging risks and recommends responses to the NRC. In addition, a Financial Risk Committee focuses on how risks impact the Deposit Insurance Fund and financial reporting.

The FDIC assesses risk-based insurance premiums by assigning a risk classification to each insured institution. The risk classifications are adjusted periodically to reflect the relative risk posed by institutions. Accordingly, institutions that represent greater supervisory risks to the insurance funds pay

higher premiums, subject to the statutory requirements.

In fulfilling its role as insurer, the FDIC has special back-up examination authority over all insured institutions and, at times, participates in examinations with the other federal regulators. In order to prevent or minimize losses to the funds, the primary federal regulator is required to take prompt corrective action when an FDIC-insured institution is determined to have capital problems. Depending on the institution's capital classification, these actions range from imposing restrictions or requirements on an institution's operations to the appointment of a receiver or conservator.

The consolidation of the banking industry has resulted in fewer and fewer financial institutions controlling an ever expanding percentage of the Nation's financial assets. As of June 30, 2006, the 10 largest FDIC-insured institutions controlled 44 percent of total insured assets and 42 percent of total insured deposits in the country. The FDIC is the primary federal regulator for none of these large financial institutions. In recent years, the FDIC has taken a number of measures to strengthen its oversight of the risks to the insurance fund posed by the largest institutions, and its key programs include the following:

- Large Insured Depository Institution Program,
- Dedicated Examiner Program,
- Shared National Credit Program, and
- Off-site monitoring systems.

Our audit work in this area for 2007 envisions evaluating the Dedicated Examiner Program, a program that the FDIC uses in the six largest banks in cooperation with other primary federal regulators and bank personnel to obtain real-time access to information about risk and trends in those institutions. Also, we plan to review the FDIC's overall approach to identify and manage risks to the Deposit Insurance Fund.

Potential Outcomes

- Strengthened FDIC assessments of risks to the Deposit Insurance Fund.
- Improved external risk mitigation.

Strategic Goal 3:

The OIG will Assist the FDIC to Protect Consumer Rights and Ensure Customer Data Security and Privacy

Consumer protection laws are an important part of the safety net of America. The U.S. Congress has long advocated particular protections for consumers in relationships with banks. For example:

- The Community Reinvestment Act (CRA) encourages federally insured banks to meet the credit needs of their entire community.
- The Equal Credit Opportunity Act prohibits creditor practices that discriminate based on race, color, religion, national origin, sex, marital status, or age.
- The Home Mortgage Disclosure Act was enacted to provide information to the public and federal regulators regarding how depository institutions are fulfilling their obligations towards community housing needs.
- The Fair Housing Act prohibits discrimination based on race, color, religion, national origin, sex, familial status, and handicap in residential real-estate-related transactions.
- The Gramm-Leach-Bliley Act eliminated barriers preventing the affiliations of banks with securities firms and insurance companies and mandates new privacy rules.
- The Truth in Lending Act requires meaningful disclosure of credit and leasing terms.
- The Fair and Accurate Credit Transaction Act further strengthened the country's national credit reporting system and assists financial institutions and consumers in the fight against identity theft.

The FDIC serves a number of key roles in the financial system and among the most important is the FDIC's work in ensuring that banks serve their communities and treat consumers fairly. The FDIC has recognized the importance of its role in this regard by establishing its own strategic goal ensuring that consumers' rights are protected and supervised institutions invest in their communities. The FDIC carries out its role by (1) providing consumers with access to information about their rights and disclosures that are required by federal laws and regulations and (2) examining the banks where the FDIC is the primary federal regulator to determine the institutions' compliance with laws and regulations governing consumer protection, fair lending, and community investment.

An important FDIC initiative is promoting expanded opportunities for the underserved banking population in the United States to enter the financial mainstream. Newly appointed FDIC Chairman, Sheila Bair said, "The FDIC has been a leader in financial education efforts, but more can be done. Regulators and bankers can work together to reach out to underserved communities and to develop credit and deposit products that meet the needs of those communities." The FDIC promotes public understanding of the federal deposit insurance system and seeks to ensure that depositors and bankers have ready access to information about consumer protection laws. The results of the

FDIC's efforts bring greater stability and fairness to our financial system.

The OIG's role under this strategic goal is targeting audits and evaluations that review the effectiveness of various FDIC programs aimed at protecting consumers, fair lending, and community investment. Additionally, the OIG's investigative authorities are used to identify, target, disrupt, and dismantle criminal organizations and individual operations engaged in fraud schemes that target our financial institutions.

2007 Performance Goals: To assist the FDIC to protect consumer rights and ensure customer data security and privacy, the OIG will

- Evaluate the effectiveness of FDIC programs for ensuring customer data security and privacy at FDIC-insured institutions.
- Review FDIC's examination coverage of institution compliance at FDIC-insured institutions.
- Address allegations of fraudulent insurance coverage and identity theft schemes affecting the FDIC.

2007 Performance Goal 3.1:

Evaluate the effectiveness of FDIC programs for ensuring customer data security and privacy at FDIC-insured institutions.

Key Effort

- Evaluate how the FDIC identifies offshore outsourcing activities in FDIC-supervised institutions and assesses the programs those institutions have in place to address the data security risks associated with offshore outsourcing. **[AUDIT]**
- Assess DSC's IT examination procedures for addressing the security of sensitive customer information when FDIC-supervised institutions use TSPs and examiners' implementation of those procedures. **[AUDIT]**

Significance

Data security and financial privacy are important values in American society. Banks are increasingly using third-party servicers to provide support for core information and transaction processing functions. The increasing globalization and cost saving benefits of the financial services industry are leading many banks to make greater use of foreign-based service providers. Although generally permissible, this outsourcing practice raises certain risks, such as country, compliance, contractual, and reputation risks.

With respect to privacy and security, the obligations of a financial institution to protect the privacy and security of information about its customers under applicable U.S. laws and regulations remain in full effect when the institution transfers the information to a foreign-based service provider. The transfer of that information to a service provider located in another country does not alter those obligations. Accordingly, the FDIC expects financial institutions to effectively manage these risks and adequately oversee any relationships with foreign-based third-party service providers.

Potential Outcomes

- Enhanced data security of sensitive customer information in financial institutions and protection of the FDIC's reputation for maintaining public confidence in the banking system.

2007 Performance Goal 3.2:

Review the FDIC's examination coverage of institution compliance programs at FDIC-supervised institutions.

Key Effort

- Determine whether DSC is adequately assessing financial institutions' compliance management systems during the compliance examination process. **[AUDIT]**
- Determine whether revisions to the interagency CRA regulations and examination procedures have achieved their intended purposes and assess the impact of the revised regulations and procedures on the CRA performance of FDIC-supervised institutions and how that impact is being measured by the FDIC. **[AUDIT]**

Significance

Compliance with laws and regulations must be managed as an integral part of a bank's business strategy. FDIC has responsibility for ensuring that the financial institutions it supervises comply with consumer protection laws and regulations. A compliance management system is the method by which the bank manages the entire consumer compliance process. The FDIC uses its compliance examination process to ascertain the effectiveness of an institution's program for compliance. In 2005, the FDIC conducted 2,020 compliance and CRA examinations.

Although the job of compliance has grown more complex, the FDIC is committed to making certain that financial institutions develop and maintain a sound compliance management system that is integrated into the overall risk management strategy of the institution. Noncompliance with consumer statutes and regulations can result in monetary penalties, litigation, and formal enforcement actions. Successful compliance management will avoid these potential consequences and create a culture of compliance readiness.

Potential Outcomes

- A sound compliance management system that is essential to the efficient and successful operation of an institution.

2007 Performance Goal 3.3:

Address allegations of fraudulent insurance coverage and identity theft schemes affecting the FDIC.

Key Efforts

- Conduct investigations of alleged schemes that defraud investors by misrepresenting FDIC-insurance coverage or affiliation. **[INVESTIGATION]**
- ECU will continue to work with DSC and the Computer Security Incident Response Team in detecting and investigating identity theft attempts which warrant issuance of FDIC Special Alerts to banks and consumers and will take all steps necessary to have fraudulent websites shut down; participate in the Cyberfraud Working Group, the Identity Theft Working Group, the HighTech Crimes Investigative Association; and coordinate with the Federal Trade Commission to identify and help combat emerging schemes that prey on consumers. **[INVESTIGATION]**

Significance

Every year fraud schemes rob depositors and financial institutions of millions of dollars. The OIG's Office of Investigations is used to identify, target, disrupt, and dismantle criminal organizations and individual operations engaged in fraud schemes that target our financial institutions or that prey on the banking public. OIG investigations have identified multiple schemes that defraud depositors. Common schemes range from identity fraud to Internet scams such as "phishing" and "pharming".

The misuse of the FDIC's name logo has also been identified as a scheme to defraud depositors. Such misrepresentations have led depositors to invest on the strength of FDIC insurance while misleading them as to the true nature of the investment products being offered. These depositors, who are often elderly and dependent on insured savings, have lost millions of dollars in the schemes. Depositors may be particularly attracted to these misrepresented investments in our current economy when interest paid on insured deposits is historically low and uninsured investments can put an investor's principal at substantial risk. Further, abuses of this nature may erode public confidence in federal deposit insurance.

Investigative work related to these areas is ongoing and will continue to be at the forefront of OI's key efforts. With the help of sophisticated technology, the ECU will continue to work with FDIC divisions and other federal agencies to help with the detection of new fraud patterns and combat existing fraud. Coordinating closely with the Corporation's DRR and the various U.S. Attorneys' offices, the OIG hopes to reduce substantial risk and yield positive results. These proactive measures will help to promote continued public confidence in federal deposit insurance and goodwill within financial institutions.

Table 3.1: Costs of ID Theft in 2006

Percent of Population Victimized	4.0%
Number of Victims	8.9 million
Annual Cost	$56.6 billion
Average Fraud Amount Per Case	$6,383
Average Time Victims Spent Resolving	40 hours

Source: Javelin Strategy & Research, 2006 Identity Fraud Survey Report

Potential Outcomes

- Detected and reduced incidence of fraud schemes intended to defraud depositors and undermine public confidence in deposit insurance.
- Reduced incidence of misrepresentations regarding FDIC deposit insurance.

Strategic Goal 4:

The OIG Will Help Ensure that the FDIC is Ready to Resolve Failed Banks and Effectively Manages Receiverships

The United States provides protection to depositors in its banks, savings and loan associations, and credit unions. One of the key players in this process is the FDIC. Among its various functions, the FDIC acts as the receiver or liquidating agent for failed FDIC-insured institutions. The success of the FDIC's efforts in resolving troubled institutions has a direct impact on the banking industry and on the taxpayers.

DRR exists to plan and efficiently handle the resolutions of failing FDIC-insured institutions and to provide prompt, responsive, and efficient administration of failing and failed financial institutions in order to maintain confidence and stability in our financial system.

- The **resolution process** involves valuing a failing federally insured depository institution, marketing it, soliciting and accepting bids for the sale of the institution, determining which bid to accept and working with the acquiring institution through the closing process.
- The **receivership process** involves performing the closing function at the failed bank; liquidating any remaining assets; and distributing any proceeds to the FDIC, the bank customers, general creditors, and those with approved claims.

The FDIC's resolution and receivership activities pose tremendous challenges. Today record profitability and capital in the banking industry have led to a substantial decrease in the number of financial institution failures compared to prior years. However, as indicated by the trends in mergers and acquisitions, banks are becoming more complex, and the industry is consolidating into larger organizations. As a result, the FDIC could potentially have to handle a failing institution with a significantly larger number of insured deposits than it has had to deal with in the past.

The change between how the FDIC handled resolutions and receiverships 20 years ago and how it will be handling them 20 years from now will be largely based on learning to anticipate and plan, instead of reacting. Through the development of new resolution strategies within the various DRR business lines, FDIC must set far-reaching plans for the future to keep pace with a changing industry.

The OIG's role under this strategic goal is targeting audits and evaluations that assess the effectiveness of the FDIC's various programs designed to ensure that the FDIC is ready to and does respond promptly, efficiently, and effectively to financial institution closings. Additionally, the OIG investigative authorities are used to pursue instances where fraud is committed to avoid paying the FDIC civil settlements, court-ordered restitution, and other payments as the institution receiver. The OIG will also continue to work with FDIC officials to keep abreast of the ongoing efforts being taken by DRR and the Corporation as a whole, to sustain proficiency in resolution activity and to prepare for the possibility of a large

institution failure or multiple failures caused by a single catastrophic event.

2007 Performance Goals: To help ensure the FDIC is ready to resolve failed banks and effectively manages receiverships, the OIG will:

- Evaluate the FDIC's plans and systems for managing bank resolutions.
- Respond to potential crimes affecting FDIC's efforts to recover financial losses.

2007 Performance Goal 4.1:
Evaluate the FDIC's plans and systems for managing bank resolutions.

Key Effort

- Evaluate the design and implementation of controls used by the FDIC to protect personal information collected and maintained in electronic form as a result of resolution and receivership activity. **[AUDIT]**
- Monitor DRR's planning for a potential large bank failure. **[OTHER PROJECT]**

Significance

In performing their duties of resolving failing FDIC-insured depository institutions, DRR personnel have access to a wide variety of records containing personally identifiable information of a bank's employees and customers. Such records include: bank employee payroll records, customer deposit records, and customer loan records. The FDIC is committed to protecting the privacy of personal information. Within the FDIC, each division has established controls and procedures for the protection of sensitive information. Through various policies and procedures, DRR has established certain methods for controlling access to collected and maintained sensitive information. However, given the increased risks associated with, and attention being placed on identity theft, the protection of customer information in FDIC's systems is paramount to sustaining the public's confidence in the FDIC.

The risk of a large bank failure is one of the greatest threats to the Deposit Insurance Fund and public confidence in the nation's financial systems. The FDIC bears primary responsibility to plan the government's reaction to such a failure. DRR has plans for sophisticated models to train FDIC staff and prepare for differing circumstances. The OIG will monitor the development of the model, look for opportunities to contribute, and involve its own staff in simulations of potential large bank fraud that causes a bank to collapse, and in post-failure reviews of what caused the bank to fail.

Potential Outcomes

- Help to ensure that the FDIC minimizes the risks of mishandling sensitive information in its possession that, if inappropriately released, could greatly damage its reputation and the public's confidence.
- Better preparation for a large bank failure.

2007 Performance Goal 4.2:

Respond to potential crimes affecting the FDIC's efforts to recover financial losses.

Key Efforts

- Continue criminal investigations of individuals fraudulently concealing assets from FDIC. **[INVESTIGATION]**
- Continue to respond to any bank closing where fraud is suspected to have played a role in the failure of the institution. An investigative team, to include ECU agents, will respond in the event of such a closing, and will share data imaged from the closing as needed with FDIC. **[INVESTIGATION]**
- OI will work with DRR and Legal to improve bank closing procedures for: addressing coordination issues with contractors who collect electronic data; providing immediate investigative response and coordination with the Department of Justice and the FBI to a large or multiple bank failure; and identifying and developing training that will help maintain proficiencies and expertise at bank closings. **[INVESTIGATION]**

Significance

The OIG's OI coordinates closely with DRR, with special attention to various types of financial institution fraud and related crimes, including concealment of assets. The FDIC was owed more than $1.7 billion in criminal restitution as of September 30, 2006. In most instances, the individuals do not have the means to pay. However, a few individuals do have the means to pay but hide their assets and/or lie about their ability to pay. OI works closely with DRR and the Legal Division in aggressively pursing criminal investigations of these individuals. Specifically, OI offers vital assistance in these pursuits. In the case of bank closings where fraud is suspected, OI is prepared to send case agents and computer forensic special agents from the ECU to the institution. Agents use different investigative tools to provide computer forensic support to OI's investigations by obtaining, preserving, and later examining evidence from computers at the bank. The determined investigative work of OI has allowed for successful outcomes in various cases and substantial restitution payments. As a result of well-prepared investigations, FDIC has a good recovery record of funds for the receivership.

Although there have been far fewer failures in recent years, DRR must be ready to resolve troubled institutions and is, in fact, continuing to focus on its ability to resolve institutions of any size. According to FDIC analysis, the failures of the 1980s and early 1990s were concentrated in the energy, agriculture, and commercial real estate sectors. In contrast, recent bank failures are largely attributable to fraud, mismanagement, improper accounting and reporting practices, and losses related to investments in sub-prime lending. OI will continue to work with DRR to ensure the OIG remains proficient and up-to-date on DRR's resolution strategies.

Potential Outcomes

- Debts owed to the FDIC collected.
- Justice for individuals who criminally conceal assets.
- Deterrence of those who might consider similar crimes.

Strategic Goal 5:

The OIG Will Promote Sound Governance and Effective Stewardship and Security of Human, Financial, IT, and Physical Resources

The FDIC must effectively manage and utilize a number of critical strategic resources in order to carry out its mission successfully, particularly its human, financial, IT, and physical resources. The Corporation does not receive an annual appropriation, except for its OIG, but rather is funded by the premiums that banks and thrift institutions pay for deposit insurance coverage, the sale of assets recovered from failed banks and thrifts, and from earnings on investments in U.S. Treasury securities.

The FDIC has emphasized its stewardship responsibilities for all of its resources in its strategic planning process. The FDIC Board of Directors approves an annual Corporate Operating Budget to fund the operations of the Corporation.

The Corporate Operating Budget provides resources for the operations of the Corporation's three major programs or business lines—Insurance, Supervision, and Receivership Management—as well as its major program support functions (legal, administrative, financial, IT, etc.). Program support costs are allocated to the three business lines so that the fully loaded costs of each business line are displayed in the operating budget approved by the Board.

In addition to the Corporate Operating Budget, the FDIC has a separate Investment Budget that is composed of individual project budgets approved by the Board of Directors for major investment projects. Budgets for investment projects are approved on a multi-year basis, and funds for an approved project may be carried over from year to year until the project is completed. A number of the Corporation's more costly IT projects are approved as part of the investment budget process.

Deposit insurance reform legislation resulted in the merging the Bank Insurance Fund and the Savings Association Insurance Fund into a new fund, the Deposit Insurance Fund, effective March 31, 2006. Expenditures from the Corporate Operating and Investment Budgets are paid from two funds managed by the FDIC—the Deposit Insurance Fund and the FSLIC Resolution Fund. The Corporation's 2007 spending is expected to total approximately $1 billion.

To effectively manage its budget, in May 2005, the Corporation implemented an enhanced cost-management program to provide managers with additional cost information, including the fully loaded cost of key businesses processes. The Corporation will also continue to benchmark the cost of selected business processes with those of peer organizations and continue to explore the use of performance scorecards to assess performance against appropriate cost, timeliness, quality, and customer service standards.

Financial resources are but one aspect of the FDIC's critical assets. The Corporation's **human capital** is also vital to its success. The FDIC will have the opportunity over the next decade to substantially reshape its workforce in conjunction with the projected retirements of a large number of

long-serving employees. The downsizing that has occurred over the past 12 years has resulted in limited hiring of new employees. The FDIC has made efforts over the recent years to address the need to reshape its workforce with the implementation of the Corporate Employee Program, the Succession Management Program, and the Leadership Development Program. In 2006, the Corporation began the development and implementation of a comprehensive succession management program to ensure that the FDIC's workforce has the skills and expertise needed to successfully address its mission responsibilities in the future and to maintain its leadership role in the financial regulatory community. Throughout the reshaping of its workforce, the FDIC maintains its commitment to a working environment of high integrity and to the achievement of its mission.

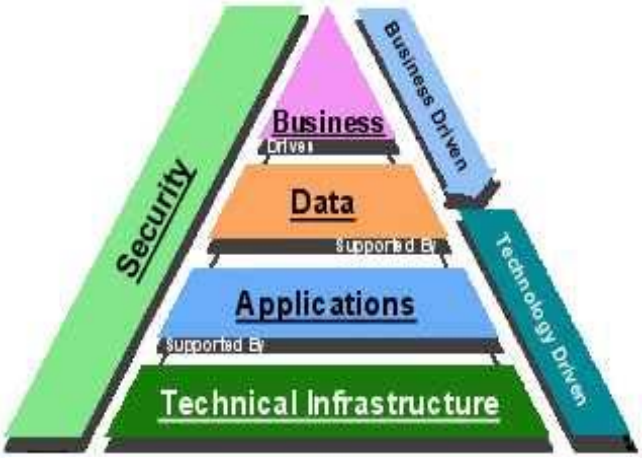
Technological advances have produced tools that all workers today would be lost without. **IT** drives and supports the manner in which the public and private sector conduct their work. At the FDIC, the Corporation seeks to leverage IT to support its business goals in insurance, supervision and consumer protection, and receivership management, and to improve the operational efficiency of its business processes. The financial services industry employs technology for similar purposes.

Along with the positive benefits that IT offers comes a certain degree of risk. In that regard, **information security** has been a long-standing and widely acknowledged concern among federal agencies. A key effort for all agencies must be the establishment of effective information security programs. The E-Government Act of 2002 recognized the importance of information security. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), requires each agency to develop, document, and implement an agency-wide information security program to provide adequate security for the information and information systems that support the operations and assets of the agency. Section 522 of the Consolidated Appropriations Act of 2005 requires agencies to establish and implement comprehensive privacy and data protection procedures and have an independent third-party review performed of their privacy programs and practices.

Business continuity is another key concern to all federal agencies. In light of recent large-scale disasters, the Corporation must be prepared to respond to such events, whether related to natural disasters or terrorism. The continuity of FDIC's business operations is essential in order to maintain the public's confidence and trust in the Corporation.

With greater uses of technological advances, the FDIC found itself with IT applications largely "stovepiped" around workgroup needs, not enterprise business needs. The stovepiped view of data in these applications made data consistency and integrity a greater challenge, according to a study published in December 2005 by Gartner, Inc. Accordingly, the FDIC has adopted an Enterprise Architecture blueprint for security and e-government as depicted in Figure 5.1.

Figure 5.1: FDIC Enterprise Architecture



Source: FDIC

The Federal Deposit Insurance Act empowers the FDIC to enter into **contracts to procure goods and services**. The authority to establish policies and procedures for the contracting program has been redelegated by the Board of Directors to the Director, Division of Administration. The Acquisition Services Branch of that Division is responsible for developing contracting policies and procedures, and communicating and implementing

those policies and procedures throughout the FDIC. Heightened corporate-wide attention to contract administration is critical to ensuring the Corporation receives cost-effective, quality performance from contractors. The FDIC is increasingly relying on contractors to accomplish its mission. The table below shows the value of active contracts by division as of March 2006.

Division	Contract Dollars (in millions)
Division of Finance	$10
Division of Insurance and Research	$39
Division of Resolutions and Receiverships	$57
Division of Administration	$284
Division of Information Technology	$1,130
Total	**$1,520**

Source: Quarterly Contracting Report to the FDIC Board of Directors

Given the sizable amount of funds committed to contracting, the FDIC has employed new strategies and controls to ensure that it maintains proper oversight for its contracts.

Enterprise risk management (ERM) is an important strategic business tool. The Treadway Commission's Committee of Sponsoring Organizations defines ERM as "a process, effected by an entity's board of directors, management, and other personnel, applied in strategy settings across the enterprise, designed to identify potential events that may adversely affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." As an integral part of its stewardship of the insurance funds, the FDIC has established a risk management and internal control program. The Office of Enterprise Risk Management (OERM) is the corporate oversight manager for internal controls and risk management. OERM works in partnership with all FDIC divisions and offices, helping them to identify, evaluate, monitor, and manage their risks.

The OIG's role in this strategic goal is to perform audits, evaluations, and investigations that

- identify opportunities for more economical, efficient, and effective corporate expenditures of funds;
- foster corporate human capital strategies that benefit employees, strengthen employees' knowledge, skills, and abilities; ensure employee and contractor integrity; and inspire employees to perform to their maximum capacity;
- help the Corporation to leverage the value of technology in accomplishing the corporate mission and promote the security of both IT and human resources;
- ensure that procurement practices are fair, efficient, effective, and economical; and
- enhance corporate governance and risk management practices.

2007 Performance Goals: To promote sound governance and effective stewardship of FDIC strategic resources, the OIG will

- Evaluate corporate efforts to fund operations efficiently, effectively, and economically.
- Assess corporate human capital strategic initiatives.
- Promote integrity in FDIC internal operations.
- Promote alignment of IT with the FDIC's business goals and objectives.
- Promote IT security measures that ensure the confidentiality, integrity, and availability of corporate information.
- Promote personnel and physical security.
- Evaluate corporate contracting efforts.
- Monitor corporate risk management and internal control efforts.

2007 Performance Goal 5.1:

Evaluate corporate efforts to fund operations efficiently, effectively, and economically.

Key Efforts

- Evaluate the effectiveness of the FDIC's records management program. **[EVALUATION]**
- Evaluate the effectiveness of FDIC's newly established Project Management Office (PMO). **[AUDIT]**
- Evaluate the appropriateness to which salary costs are being charged to various New Financial Environment (NFE) program codes. **[EVALUATION]**
- Evaluate the performance measurement processes that the FDIC uses to monitor corporate performance. **[EVALUATION]**

Significance

Records are a valuable resource and must be managed properly for the agency to function effectively and to comply with Federal laws and regulations. The FDIC records management program is designed to ensure continuity and consistency, to assist in decision-making and information-sharing, and to provide information required by Congress and others for overseeing the Corporation's activities. Thus, it is important that the Corporation's records are economically and effectively managed to meet business needs and to comply with applicable laws and regulations.

Improving project management is another ongoing business concern. In 2005, The Division of Information Technology (DIT) PMO was established as a resource center for clients, executives, project managers, and project team members engaged in the operations and oversight of IT projects. DIT initiated a PMO to establish standard repeatable project management practices and improve the results of IT project management activities. Successful project management is highly dependent upon keeping decision-makers fully informed of the cost and status of projects.

In May 2005, the Corporation also implemented NFE to enhance the FDIC's ability to meet current and future financial management and information needs. One of the intended organizational benefits of NFE was enhanced cost management. To that end, the cost management program was collaboratively created by all divisions and offices. The cost management program's success will rely on employees accurately entering all the necessary data into the appropriate cost management chartfields when reporting their time and travel. In order to facilitate and support decision making, accurate cost data must be available for decision makers and other system users.

To provide assurance that the FDIC is achieving its strategic goals and objectives, there must be gauges that track and measure the Corporation's performance of its operations, activities, and initiatives. Furthermore, these gauges must be aligned with the Corporation's strategic goals and objectives and be useful to FDIC management and stakeholders.

Potential Outcomes

- Enhanced usefulness and reliability of records for decision makers.
- Cost-effective records management processes.
- Enhanced project management practices.

- Accurate cost data for decision makers and other system users.
- Performance measures that appropriately assess the Corporation's performance and are useful to FDIC management and stakeholders.

2007 Performance Goal 5.2:

Assess corporate human capital strategic initiatives.

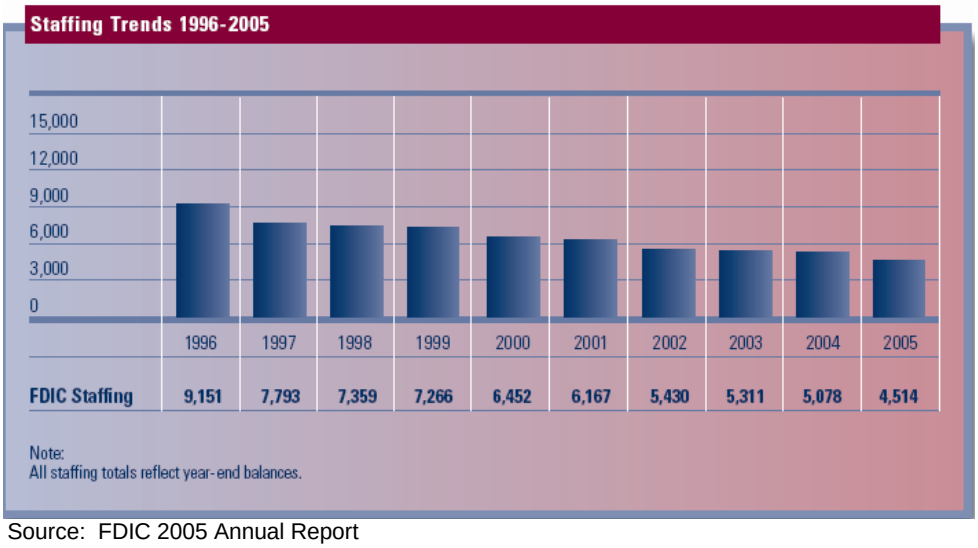
Key Efforts

- Determine the extent to which the FDIC's succession planning efforts identify and address future critical staffing and leadership needs. **[EVALUATION]**
- Evaluate the efficiency, effectiveness, and customer satisfaction with FDIC's hiring program, procedures, and processes. **[EVALUATION]**

Significance

Federal agencies are faced with a growing number of employees who are eligible for retirement and are finding it difficult to fill certain mission-critical jobs— a situation that could significantly drain agencies' institutional knowledge. To that end, the FDIC established a new human capital framework and strategy to guide its planned evolution toward a more flexible permanent workforce that will be capable of responding rapidly to significant changes in the financial services industry or unexpected changes in workload or priorities. As depicted in Figure 5.2, over the past 10 years the Corporation was in a continuous downsizing mode as it completed the residual workload from the banking and thrift crises of the late 1980s and early 1990s but expects that significant downsizing activity is now complete. The FDIC is now reshaping its workforce to better align it with anticipated future human resource requirements. To help facilitate this transition, the FDIC implemented a tool, FDIC Careers, a fully automated hiring system in 2004, to make it easier for the FDIC to attract, screen and hire new employees. Given the importance of attracting, maintaining, and developing a solid workforce, the Corporation needs to ensure that is it employing effective and efficient methods and tools to meet the human capital needs of the Corporation.

Figure 5.2: Corporate Staffing



Source: FDIC 2005 Annual Report

Potential Outcomes

- Increased assurance that future leaders have the skills and expertise needed to carry out the FDIC mission.
- A more effective and efficient program for attracting, screening, and hiring new employees.

2007 Performance Goal 5.3:
Promote integrity in FDIC internal operations.

Key Efforts

- Conduct investigations, as needed, of criminal or serious misconduct on the part of FDIC employees and contractors to ensure a working environment of high integrity. **[INVESTIGATION]**
- Electronic Crimes Unit collaboration with the FDIC to ensure appropriate use of government property. **[INVESTIGATION]**
- Maintain OIG Hotline to respond to allegations of fraud, waste, abuse, and mismanagement. **[INVESTIGATION]**
- Participate with FDIC Ethics Office in addressing employee groups on ethics and conduct issues. **[INVESTIGATION]**

Significance

The achievement of the FDIC's mission, in large part, depends upon employees that uphold values of integrity, honesty, and a commitment to maintain the public's trust and confidence in the Corporation. In order to promote a working environment that embraces such values, there must be means in which misconduct is identified and handled appropriately. To foster a working environment of high integrity, it is also critical that employees and contractors receive ethics and conduct training.

Potential Outcomes

- Heightened awareness of unacceptable or unethical employee behavior and the appropriate consequences for such behavior.
- Appropriate use of resources for intended purposes.
- A working environment of high integrity.

2007 Performance Goal 5.4:
Promote alignment of IT with the FDIC's business goals and objectives.

Key Efforts

- Assess the FDIC's progress in implementing an enterprise architecture program that supports the FDIC's mission. **[AUDIT]**
- Complete a risk assessment of FDIC's IT environment, including corporate risk mitigation activities. **[AUDIT]**

Significance

An Enterprise Architecture (EA) is a blueprint of an agency's current and planned operating and systems environment and the plan for transitioning between the two. Among other things, the EA defines principles and goals for, and sets direction on, IT security. It is critical that the FDIC has an effective structure in place to allow IT investment decisions to be made in alignment with its business needs; otherwise, the absence of an effective EA program may result in poor IT investment decisions.

As part of the OIG's approach to assess the FDIC's IT environment and risk, the OIG will conduct a risk analysis of FDIC's IT environment to ensure that resources are focused on areas that represent the most risk to the FDIC.

Potential Outcomes

- Assurance that FDIC has an effective structure in place to allow IT investment decisions to be made in alignment with its business needs.
- Assurance that resources are devoted to areas that represent most risk to the FDIC.

2007 Performance Goal 5.5:

Promote IT security measures that ensure the confidentiality, integrity, and availability of corporate information.

Key Efforts

- Evaluate the effectiveness of the FDIC's information security and privacy and data protection program and practices, including the FDIC's compliance with FISMA and related policies, procedures, standards, legislation, and guidelines. **[AUDIT]**
- Determine whether the FDIC has established and implemented an IT disaster recovery capability that is consistent with federal standards, guidelines, and industry-accepted practices. **[AUDIT]**
- Evaluate the Corporation's use of information in identifiable form, evaluate the privacy and data protection procedures, and recommend strategies and specific steps to improve data protection management. **[AUDIT]**

Significance

Information security and continuity of operations remain top priorities at the FDIC. As mandated by Title III, namely FISMA, of the *E-Government Act of 2002*, federal agencies are required to have an annual independent evaluation performed of their information security programs and practices and to report the results of the evaluation to the Office of Management and Budget (OMB). The OIG's 2006 FISMA evaluation reported that the FDIC has made significant progress in improving its information security controls and practices. However, continued management attention was needed in key security control areas to ensure that appropriate risk-based and cost-effective security controls are in place to secure the FDIC's information resources in

furtherance of the Corporation's security program goals and objectives. Further, the Corporation is subject to the Consolidated Appropriations Act, Title V, Section 522. The Act mandates the designation of a senior privacy official, establishment of privacy and data protection procedures, and a written report of the Corporation's use of information in identifiable form.

The FDIC depends on the continuity of its IT operations to meet its business needs, financial obligations, and regulatory requirements. OMB policy requires agencies to establish and periodically test their ability to recover from IT service interruptions and to provide service based upon the needs and priorities of system participants. The FDIC conducts semiannual IT disaster recovery testing to ensure the Corporation's ability to recover its mainframe, midrange, and server platforms that would be required to restore IT operations in the event of a disaster. It is of critical importance that the FDIC IT infrastructure can withstand interruptions and continue to fully support corporate business operations.

Potential Outcomes

- Strengthened, up-to-date information and system security controls and practices.
- Appropriate use of information in an identifiable form and enhanced protection of sensitive data.
- A reliable IT disaster recovery capability.

2007 Performance Goal 5.6:
Promote personnel and physical security.

Key Effort

- Determine the extent of the FDIC's progress in developing and implementing a comprehensive business continuity plan (BCP) and program. **[AUDIT]**

Significance

Recent large-scale disasters in the United States have clearly demonstrated how important it is to have reliable emergency response procedures and a well-written BCP to sustain critical business functions during an emergency or situation that may disrupt normal operations. The FDIC has developed an Emergency Operations Plan comprised of an Emergency Response Plan and a separate BCP. In 2004, an OIG evaluation of FDIC's BCP found that the BCP addresses the critical business functions of key FDIC divisions and offices. However, the evaluation noted that the FDIC could improve the quality of its BCP in a number of key areas to help ensure its success. The OIG will conduct a follow-up evaluation of the FDIC's progress in implementing the recommendations we made in our earlier report. It is important, both symbolically and functionally, for federal government agencies to continue to serve the American public during any emergency or situation that may disrupt normal operations.

Potential Outcomes

- A sound BCP that helps ensure public confidence in the FDIC and its regulated banks.

2007 Performance Goal 5.7:
Evaluate corporate contracting efforts.

Key Efforts

- Assess whether the FDIC has mechanisms in place to periodically evaluate the continuing need for contracts and determine whether there are corporate contracts that can be eliminated. **[EVALUATION]**
- Determine whether the Information Technology Application Services (ITAS) contracting approach is achieving anticipated procurement benefits, and (2) ascertain whether there is an appropriate balance between the controls in place and the risks inherent in the ITAS contracting approach. **[EVALUATION]**
- Determine whether adequate controls to ensure that work performed under the Federal Systems Integration Management (FEDSIM) interagency agreement contract complies with contract's terms and conditions, and the contracting method has produced the intended results. **[AUDIT]**
- For pre-award reviews—determine whether the FDIC is complying with its Acquisition Policy Manual in evaluating proposals and/or assess financial aspects of bidders' proposals, including determining whether proposed costs are reasonable and supported. **[EVALUATION]**
- For contract billing reviews—determine whether contractor billings are allowable under the contract, allocable, and reasonable. **[EVALUATION]**

Significance

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 contract award must be in place and work effectively. As a good steward, the FDIC must ensure it receives the goods and services purchased with corporate funds. Further, the FDIC must have mechanisms in place to periodically evaluate the continuing need for contracts and determine whether there are corporate contracts that can be eliminated.

In 2004, the Corporation initiated a new contracting approach for its IT services with the goal to improve contractor support and streamline procurement and oversight activities. The ITAS contract combined approximately 40 contracts into one contract with multiple (four) vendors for a total program value of $555 million over 10 years. In such a large contractual undertaking, significant risk may exist in getting work completed, overseeing the contract, and, ultimately, meeting the Corporation's needs. In addition, in 2004, the FDIC entered into an interagency agreement with the General Services Administration—FEDSIM contract—to provide assistance for IT support services. As of June 2005, a Contract Monitoring

Information Application report indicated that the FEDSIM contract totaled $342 million. Considering the significant contract cost and the vital IT functions that are being acquired, the success of the FEDSIM contract will be extremely important to the FDIC for many years to come.

Potential Outcomes

- Cost savings from optimizing contract portfolios and consolidating redundant contracts.
- Strengthened contract administration and cost savings.
- Assurance that the ITAS and FEDSIM contracts are meeting the FDIC's IT infrastructure and development needs.

2007 Performance Goal 5.8:

Monitor corporate risk management and internal control efforts.

Key Effort

- Determine the extent to which the FDIC has implemented its Enterprise Risk Management Program consistent with applicable government-wide and best practices. **[EVALUATION]**

Significance

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.

Potential Outcomes

- An enterprise-wide control environment that strikes the right balance of internal controls and corporate risks.
- Clear definition of responsibility for addressing corporate risks.

Strategic Goal 6:

The OIG Will Build and Sustain a High-Quality OIG Work Environment

While the purpose of the OIG is focused on the FDIC's programs and operations, we have an inherent obligation to hold ourselves to the highest standards of performance and conduct. Like any organization, we have processes and procedures for conducting our work; communicating with our clients, staff, and stakeholders; managing our financial resources; aligning our human capital to our mission; strategically planning and measuring the outcomes of our work; maximizing the cost-effective use of technology; and ensuring our work products are timely, value-added, accurate, and complete and meet applicable professional standards.

2007 Performance Goals: To build and sustain a high-quality OIG work environment, the OIG will

- Encourage individual growth through personal development;
- Strengthen human capital management and leadership development;
- Foster good client, stakeholder, and staff relationships;
- Ensure quality and efficiency of OIG audits, evaluations, investigations, and other operations;
- Enhance strategic and annual performance planning and performance measurement; and
- Invest in cost-effective and secure IT.

2007 Performance Goal 6.1:

Encourage individual growth through professional development.

Key Efforts

- Develop training and development plans for auditors, evaluators, and investigators. **[INTERNAL IMPROVEMENT]**
- Conduct OIG-wide conference. **[OTHER PROJECT]**
- Explore expanding the pilot internal mentoring program. **[INTERNAL IMPROVEMENT]**
- Encourage staff to attain relevant professional certifications.
- Host an emerging issues symposium. **[OTHER PROJECT]**

Significance

The OIG's performance and value to our clients and stakeholders is directly linked to the knowledge and abilities of our staff. As our individual and collective abilities increase, so do the performance capacity of our organization and value to clients and stakeholders.

To ensure a high-quality work environment, we must continuously invest in keeping staff knowledge and skills at a level equal to the work that needs to be done. Training and development plans are one means for ensuring that the OIG is making sound investments in staff development. While each staff member has the primary responsibility for managing his or her career, OIG supervisors and management play a key role in helping staff create and implement career development plans. An emerging issues symposium is one means of keeping OIG staff attuned to changes in the bank regulatory environment. Also, a mentoring program that has been piloted during the past year may be beneficial to provide career and developmental guidance to some OIG staff.

In addition, relevant professional certifications serve to enhance the expertise of OIG staff and help ensure continued high-quality work and products.

Potential Outcomes

- Continuous improvement in OIG expertise that can match the needs of our workload.
- A workforce that can develop to its fullest potential.

2007 Performance Goal 6.2:

Strengthen human capital management and leadership development.

Key Efforts

- Include leadership development as a component of the auditor, evaluator, and investigator training plans. **[INTERNAL IMPROVEMENT]**
- Develop a pilot effort for end-of-assignment performance reviews. **[INTERNAL IMPROVEMENT]**
- Award a contract for supplemental expertise for audits, evaluations, investigations, and other OIG activities. **[INTERNAL IMPROVEMENT]**
- Update business continuity and emergency preparedness plans. **[INTERNAL IMPROVEMENT]**
- Update OIG workforce data for human capital decision-making. **[INTERNAL IMPROVEMENT]**

Significance

A committed leadership team is essential to our strategic goal to build and sustain a high-quality work environment. Leadership fosters accountability for reaching results-oriented goals and for continuous learning and improvement. The OIG needs to develop its leaders for succession to sustain its effectiveness and excellence even as current leaders may depart. Leadership development needs to occur for all employees and with each employee striving to enhance his or her leadership competencies.

OIG leaders must provide straightforward, honest, and constructive feedback about individual and organizational performance to employees. To that

end, we will develop additional tools and processes to add to the frequency and quality of performance feedback.

Our staff is our most important asset. The OIG's ability to produce products and serve clients and stakeholders is directly linked to the quality of staff. Complementing our workforce are contracted staff that can provide expertise beyond what we possess. Such experts can include contractors with expertise in IT, business continuity planning, forensic accounting, human capital issues, corporate investment strategy, commercial real estate appraisals, actuarial science, or any number of areas that OIG work may address. We will be awarding a contract in the next year to complement our existing workforce and assist us to build more quality into our work products.

Protecting our workforce in the event of any emergency is one of the highest priorities. Our emergency preparedness plan, prepared in conjunction with the FDIC's plan, aims to guide us on what to do before, during, and after an emergency and ensure the safety and security of all OIG staff. The BCP looks toward resuming, first, critical operations, and then all operations after a significant disruption. We must keep these plans current and ready for immediate implementation.

Finally, information about our workforce can guide us in making strategic decisions. We continuously monitor information about the retirement eligibility of our workforce, its demographics, and grade structure for strategic decision-making, recruitment needs, and economy and efficiency. The composition of the OIG workforce changes significantly every year as do the workload needs. We aim to collect data that assist in managing the workforce to meet the strategic needs.

Potential Outcomes

- A stronger leadership team.
- Successful leadership succession.
- A high-quality, high-performance culture.
- Enhanced expertise on OIG audits, evaluations, investigations, and projects.
- Improved readiness in the event of an emergency.

2007 Performance Goal 6.3:

Foster good client, stakeholder, and staff relationships.

Key Efforts

- Continue communications with congressional clients to keep them fully and currently informed about OIG work and issues, problems, and deficiencies relating to FDIC programs and operations.
- Complete and coordinate OIG congressional communications protocols. **[INTERNAL IMPROVEMENT]**
- Strengthen efforts to keep the FDIC Chairman, Vice Chairman, and other FDIC officials, as appropriate, fully and currently informed about OIG work and issues, problems, and deficiencies relating to FDIC programs and operations. **[OTHER PROJECT]**
- Participate with other OIGs in the President's Council on Integrity and Efficiency (PCIE) and meet with other accountability and law enforcement organizations. **[OTHER PROJECT]**

- Continue efforts to provide forums for OIG staff to address concerns, provide ideas for continuously improving the OIG, and add value to OIG products and services, including formation of the Employee Advisory Group. **[OTHER PROJECT]**
- Make OIG products accessible to the extent possible with consideration given to data sensitivity and privacy.

Significance

The Inspector General Act of 1978 (IG Act), as amended, makes the OIG responsible for keeping both the FDIC Chairman and the Congress fully and currently informed about problems and deficiencies relating to FDIC programs and operations. This dual reporting responsibility is the framework within which IGs perform their functions, and serves as a legislative safety net that protects the OIG's independence and objectivity.

The OIG places a high priority on maintaining positive relationships with the Congress and providing timely, complete, and high quality responses to congressional inquiries. Communications with the Congress about OIG work and its conclusions are best handled by the Inspector General or a designee to ensure that information is conveyed accurately and in context. In most instances, this communication would include semiannual reports to the Congress, letters for reporting serious problems, issued audit and evaluation reports, information related to completed investigations, comments on legislation and regulations, written statements for congressional hearings, contacts with congressional staff, responses to congressional correspondence, and materials related to OIG appropriations.

The OIG also places a high priority on maintaining positive relationships with the Chairman, other FDIC Board members, and FDIC officials. The OIG regularly communicates with the Chairman and Vice Chairman through briefings about ongoing and completed audits, evaluations, and investigations. The OIG is a regular participant at Audit Committee meetings where recently issued audit and evaluation reports are discussed. Other meetings occur throughout the year as OIG officials meet with division and office leaders and attend/participate in internal FDIC conferences. The OIG's semiannual reports to the Congress are sent to the Chairman 30 days prior to their transmittal to the Congress.

To assist the Congress and our other clients, many OIG products are available from the OIG's Internet site, www.fdicig.gov. These include most audit and evaluation reports, unless security issues are involved. OIG investigations are generally unavailable on the Internet due to the privacy issues involved for the subjects and witnesses of the investigations. However, press releases, usually written by the Department of Justice, concerning investigations are available on our Internet site. In addition, testimony, plans, semiannual reports to the Congress, and other documents are also available.

The IGs appointed by the President and confirmed by the Senate are members of the PCIE. The FDIC OIG fully supports and participates in PCIE activities. This organization

- addresses integrity, economy, and effectiveness issues that transcend individual Government agencies; and
- increases the professionalism and effectiveness of OIG personnel throughout the Government.

Additionally, the OIG routinely meets with representatives of the Government Accountability Office (GAO) to coordinate work and minimize duplication of effort. The OIG also meets with representatives of the Department of Justice, including the FBI and U.S. Attorneys' Offices to coordinate our criminal investigative work and pursue matters of mutual interest. Regular meetings are held with the financial regulatory OIGs and other groups where the OIG has similar business interests.

The OIG has been working over several years to be a results-oriented, high performance culture. The organization that has been envisioned would foster a work environment in which honest two-way communication and fairness are a hallmark, perceptions of unfairness are minimized, and any workforce disputes are resolved by fair and efficient means. The ideas of staff at all levels are to be sought and valued as we strive to continuously enhance OIG operations. An Employee Advisory Group, made up of elected and/or appointed OIG staff, meets regularly and provides advice to the Inspector General on a wide variety of issues in a non-threatening environment. A Diversity Coordinator also helps promote corporate diversity initiatives in our workplace.

Potential Outcomes

- Improved communications and working relationships with the OIG's clients and stakeholders.
- Increased access to OIG products.
- Increased transparency about how the OIG does its work.
- Effective coordination and cooperation with other OIGs, GAO, and other law enforcement organizations.
- A more satisfied and motivated OIG workforce.

2007 Performance Goal 6.4:

Ensure the quality and efficiency of OIG audits, evaluations, investigations, and other operations.

Key Efforts

- Review audit assignment management controls. **[INTERNAL IMPROVEMENT]**
- Update audit policies in accordance with revised *Government Auditing Standards*. **[INTERNAL IMPROVEMENT]**
- Host an external peer review of the Office of Audits and resolve any significant matters identified.
- Conduct an external peer review of another OIG. **[OTHER PROJECT]**
- Conduct periodic internal reviews of audit and investigation operations.
- Develop a project management tracking and reporting process for internal OIG projects. **[INTERNAL IMPROVEMENT]**

Significance

To carry out its responsibilities, the OIG must be professional, independent, objective, fact-based, nonpartisan, fair, and balanced in all its work. Also, the Inspector General and OIG staff must be free both in fact and in appearance from personal, external, and organizational impairments to their independence. The OIG adheres to the *Quality Standards for Federal Offices of Inspector General*, issued by the PCIE and the Executive Council on Integrity and Efficiency (ECIE). Further the OIG conducts its audit work in accordance with generally accepted *Government Auditing Standards*; its evaluations in accordance with PCIE Quality Standards for Inspectons; and its investigations, which often involve allegations of serious wrongdoing that may involve potential violations of criminal law, in accordance with *Quality Standards for*

Investigations established by the PCIE and ECIE, and procedures established by the Department of Justice.

The *Government Auditing Standards* and PCIE/ECIE standards require organizations conducting audit and investigative work in accordance with the standards to have appropriate internal quality control systems in place and undergo an external quality control review. The external quality control reviews are conducted once every 3 years by an organization not affiliated with the OIG. The FDIC OIG is a member of the PCIE, and other member organizations conduct the external quality control review on a planned schedule. Similarly, the FDIC OIG has agreed to conduct an external quality control review on another office. A reviewing organization cannot be reviewed by an organization that it has reviewed during the 3-year cycle.

Potential Outcomes

- Assurance that the OIG's internal quality control systems are in place and operating effectively to provide reasonable assurance that established policies and procedures and applicable professional standards are followed.
- Recommendations from the peer reviews that can be considered for improving OIG quality control.
- FDIC OIG observations of another OIG's practices that can be used to improve FDIC OIG operations.
- More efficient OIG business processes.

2007 Performance Goal 6.5:

Enhance strategic and annual planning and performance measurement.

Key Efforts

- Continue with an outcome-oriented strategic and annual plan with performance targets for the OIG for FY 2008. **[INTERNAL IMPROVEMENT]**
- Continuously assess and monitor changes in risk conditions that affect OIG business practices.

Significance

The FDIC OIG has its own strategic and annual planning processes independent of the Corporation's planning process, in keeping with the independent nature of the OIG's core mission. The Government Performance and Results Act of 1993 (GPRA) was enacted to improve the management, effectiveness, and accountability of federal programs. GPRA requires most federal agencies, including the FDIC, to develop a strategic plan that broadly defines the agency's mission and vision, an annual performance plan that translates the vision and goals of the strategic plan into measurable objectives, and an annual performance report that compares actual results against planned goals.

The OIG strongly supports GPRA and is fully committed to applying its principles of strategic planning and performance measurement and reporting to our operations. Doing so will enable us to focus energy on providing value to the Corporation and will help identify where changes

are needed to improve organizational effectiveness and efficiency. The OIG Strategic Plan and Annual Performance Plan lay the basic foundation for establishing goals, measuring performance, and reporting accomplishments consistent with the principles and concepts of GPRA.

Unlike the FDIC, which reports on a calendar year basis, the OIG receives a separate appropriation based on the typical government fiscal year ending September 30. Therefore, our performance planning and reporting is done on a September 30 fiscal year cycle. The fiscal year cycle is also consistent with the semiannual reporting periods prescribed by the Inspector General Act.

Past OIG strategic and performance plans sought to define many goals and objectives in quantifiable terms. To act as a catalyst in determining how the OIG directs its work and manages its resources, the OIG developed a new strategic plan framework in 2006 that adds qualitative performance measures to a few key quantitative performance measures. Collectively, these measures will help to demonstrate the degree to which the OIG's work provides timely, quality service to the Chairman, the Congress, the banking industry, and the public. Additionally, the OIG will be capable of integrating its planning, budgeting, and performance reporting to show better the relationship between resource requests and desired performance levels.

As a corollary, the OIG recognizes that internal controls and systems are important components in the design and implementation of practices for accomplishing strategic and performance goals. Consequently, continuous assessments of risks and the internal controls in place to manage the risks are part of the OIG's business strategies.

Potential Outcomes

- Ability to measure the OIG's performance and compare it to goals and results.
- Work that meets the needs of FDIC management and the Congress and facilitates improvements in FDIC programs and operations.
- Clear communication to OIG clients, stakeholders, and staff about why the OIG performs its work and what outcomes it aims to achieve and does achieve.
- Continued improvement to the OIG's strategic planning, budgeting, and productivity.
- Cost-effective internal controls that achieve internal control objectives and effectively manage risks.

2007 Performance Goal 6.6:

Invest in cost-effective and secure information technology.

Key Efforts

- Update the OIG IT Strategic Plan to guide OIG business decisions, priorities, and resource allocations for 2008-2010. **[INTERNAL IMPROVEMENT]**
- Continue enhancing the security of OIG information in the FDIC computer network infrastructure. **[INTERNAL IMPROVEMENT]**

- Invest in modern laptop computers with enhanced security. **[INTERNAL IMPROVEMENT]**
- Evaluate other IT equipment and software needs and their cost effectiveness. **[INTERNAL IMPROVEMENT]**
- Review audit and evaluation information system options and requirements for efficiency and security. **[INTERNAL IMPROVEMENT]**
- Update the OIG training system to be more efficient monitoring continuing professional education requirements. **[INTERNAL IMPROVEMENT]**
- Update the Dashboard to incorporate FY 2007 Business Plan goals and key efforts. **[INTERNAL IMPROVEMENT]**

Significance

IT has become an essential component of almost every OIG business process. It has been one factor in the OIG's ability to downsize staff by one-third since fiscal year 2003. As a component of the FDIC, the OIG receives and will continue to receive support and services offered throughout the Corporation. Where operational independence is necessary to ensure completion of the OIG mission, the OIG independently undertakes IT initiatives as needed. For instance, OIG staff are connected to the FDIC computer network and carry out day-to-day functions within the Corporation's firewall protections. In other areas, the OIG needs more independence. For example, we manage our own Internet site and content to ensure timely and complete dissemination of appropriate information.

The increasing capabilities of network administrators in the FDIC's system architecture necessitates certain security enhancements for OIG information within the network. After consultations with FDIC's DIT, the OIG will strengthen and enhance security and operational controls over network equipment and procedures to protect OIG information better.

The OIG also develops and maintains information systems that track the status of ongoing audits, evaluations, and investigations to help ensure the timeliness of our work and monitor our performance. With an updated planning, reporting, performance measurement, and budgeting process being planned, the supporting information systems need to be updated to integrate these business processes.

The OIG continuously looks for opportunities for improving our security, performance, and productivity with cost-effective computer equipment and software.

Potential Outcomes

- More integrated planning, performance measurement, reporting, and budget systems that enhance decision-making.
- Sensitive information better safeguarded.
- More productive and efficient workforce.

Quantitative Performance Measures and Targets

The table below presents our FY 2007 targets for our quantitative performance measures. The table also reflects our performance during the last three fiscal years for these measures, where available. To establish targets for these measures, we examined what we have been able to achieve in the past and the external factors that influence our work, such as budgetary resources and staffing levels.

OIG staffing and budgets, after adjusting for inflation, have continuously decreased during the past decade in response to changes in the banking industry and the FDIC. Consequently, some performance targets are lower than previous years' actual accomplishments to reflect the reduced work and staffing.

OIG Quantitative Performance Measures and Targets

Performance Measure	FY 2004 Actual	FY 2005 Actual	FY 2006 Actual	FY 2007 Target
Financial Benefit Return[a]	345%	155%	196%	100%
Other Benefits[b]	N/A	N/A	107	100
Past Recommendations Implemented[c]	N/A	N/A	87%	95%
Audit/Evaluation Reports Issued	48	40	26	26
Audit/Evaluation Assignments Completed within 30 days of Established Milestones	N/A	N/A	N/A	90%
Investigation Actions[d]	101	132	169	120
Closed Investigations Resulting in Reports to Management, Convictions, Civil Actions, or Administrative Actions	77%	84%	84%	80%
Investigations Accepted for Prosecution Resulting in Convictions, Pleas, and/or Settlements	70%	80%	67%	70%
Investigations Referred for Prosecution or Closed Within 6 Months of Opening Case	N/A	N/A	N/A	85%
Closing Reports Issued to Management within 30 days of Completion of all Judicial Actions	N/A	N/A	N/A	100%

[a] Includes all financial benefits, including audit-related questioned costs; recommendations for better use of funds; and investigative fines, restitution, settlements, and other monetary recoveries divided by OIG's total fiscal year budget obligations.

[b] Benefits to the FDIC that cannot be estimated in dollar terms which result in improved services; statutes, regulations, or policies; or business operations and occurring as a result of work that the OIG has completed over the past several years. Includes outcomes from implementation of OIG audit/evaluation recommendations.

[c] Fiscal year 2005 recommendations implemented by fiscal year-end 2007.

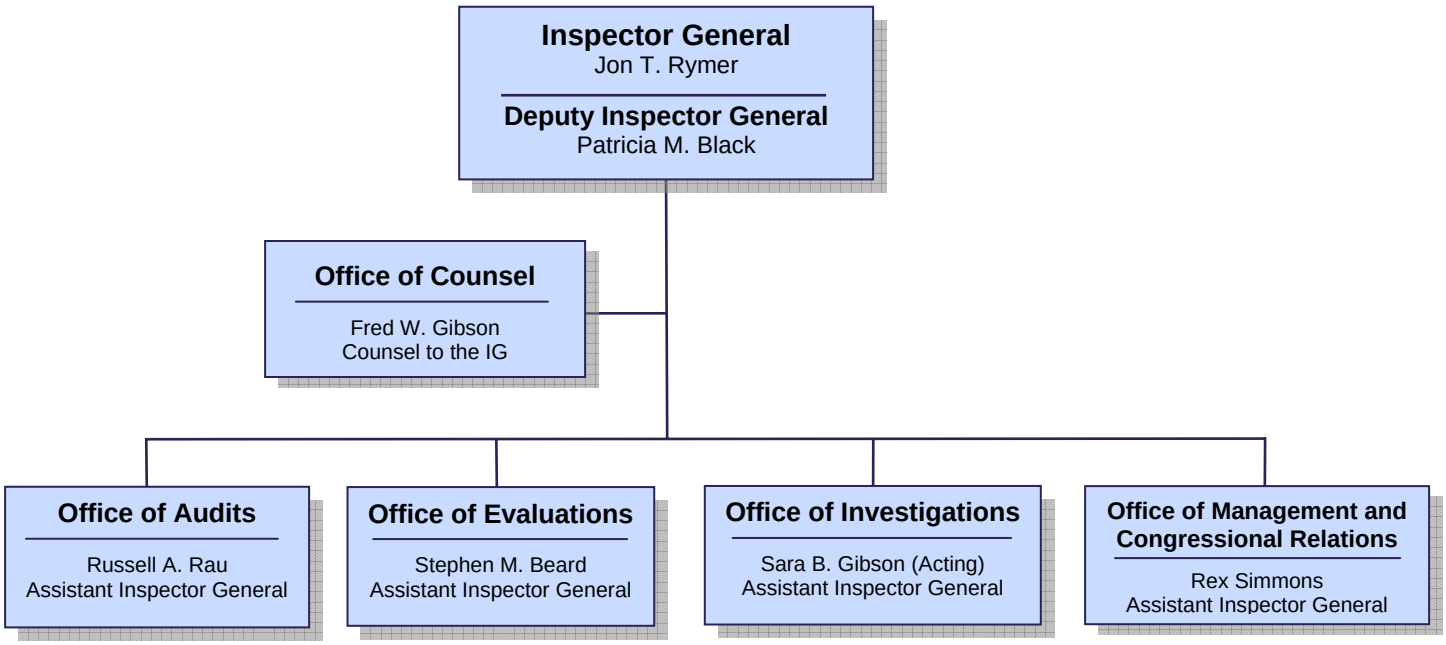
[d] Indictments, convictions, informations, arrests, pre-trial diversions, criminal non-monetary sentencings, monetary actions, employee actions, and other administrative actions.

APPENDIX I

OIG Organization Structure

The FDIC OIG is comprised of five component offices as shown below. A brief description of the duties and responsibilities of each office is also shown.

OIG Organization Chart



Office of Audits

The Office of Audits provides the FDIC with professional audit and related services covering the full range of its statutory and regulatory responsibility, including major programs and activities. These audits are designed to promote economy, efficiency, and effectiveness and to prevent fraud, waste, and abuse in corporate programs and operations. This office ensures the compliance of all OIG audit work with applicable audit standards, including those established by the Comptroller General of the United States. It may also conduct external peer reviews of other OIG offices, according to the cycle established by the PCIE.

The Office of Audits is organized into two primary Directorates: (1) Insurance, Supervision, and Receivership Management Audits and (2) Systems Management and Security Audits.

Office of Evaluations

The Office of Evaluations evaluates, reviews, studies, or analyzes FDIC programs and activities to provide independent, objective information to facilitate FDIC management decision-making and improve operations. Evaluation projects are conducted in accordance with the *PCIE Quality Standards for Inspections.* Evaluation projects are generally limited in scope and may be requested by the FDIC Board of Directors, FDIC management, or the Congress.

Office of Investigations

The Office of Investigations (OI) carries out a comprehensive nationwide program for the prevention, detection, and investigation of criminal or otherwise prohibited activity that may harm or threaten to harm the operations or integrity of the FDIC and its programs. OI maintains close and continuous working relationships with the U.S. Department of Justice; the Federal Bureau of Investigation; other Offices of Inspector General; and federal, state and local law enforcement agencies. OI coordinates closely with the FDIC's Division of Supervision and Consumer Protection in investigating fraud at financial institutions, and collaborates with the Division of Resolutions and Receiverships and the Legal Division in investigations involving failed institutions and fraud by FDIC debtors.

In addition to its two regional offices, OI operates an Electronic Crimes Unit and forensics laboratory in Washington, D.C. The Electronic Crimes Unit is responsible for conducting computer-related investigations impacting the FDIC and providing computer forensic support to OI investigations nationwide. OI also manages the OIG Hotline for employees, contractors, and others to report instances of suspected fraud, waste, abuse, and mismanagement within the FDIC and its contractor operations via a toll-free number or e-mail.

Office of Management and Congressional Relations

The Office of Management and Congressional Relations is the management operations arm of the OIG with responsibility for providing business support for the OIG, including financial resources, human resources, and IT support; strategic planning and performance measurement; internal controls; coordination of OIG reviews of FDIC proposed policy and directives; OIG policy development; and congressional relations.

Office of Counsel

The Office of Counsel to the Inspector General is responsible for providing independent legal services to the Inspector General and the managers and staff of the OIG. Its primary function is to provide legal advice and counseling and interpret the authorities of, and laws related to, the OIG. The Counsel's office also provides legal research and opinions; reviews audit and investigative reports for legal considerations; represents the OIG in personnel-related cases; coordinates the OIG's responses to requests and appeals made pursuant to the Freedom of Information Act and the Privacy Act; prepares Inspector General subpoenas for issuance; and reviews draft FDIC regulations and draft FDIC and OIG policies and proposed or existing legislation, and prepares comments when warranted; and coordinates with the FDIC Legal Division when necessary.

APPENDIX II

Resource Allocation by Strategic Goal

The table below summarizes the OIG's FY 2007 budgetary resources and the associated human capital resources in terms of full-time equivalent (FTE) positions by strategic goal.

FY 2007 Resources by Strategic Goal

Strategic Goal	Amount	Percent	FTEs	Percent
Strategic Goal 1: Assist the FDIC to Ensure the Nation's Banks Operate Safely and Soundly	$9,984,000	39%	56	43%
Strategic Goal 2: Help the FDIC Maintain the Viability of the Insurance Fund	$1,143,000	4%	6	5%
Strategic Goal 3: Assist the FDIC to Protect Consumer Rights and Ensure Customer Data Security and Privacy	$2,112,000	8%	10	8%
Strategic Goal 4: Help Ensure that the FDIC is Ready to Resolve Failed Banks and Effectively Manages Receiverships	$941,000	4%	2	2%
Strategic Goal 5: Promote Sound Governance and Effective Stewardship of Human, Financial, IT, and Physical Resources	$9,083,000	35%	45	34%
Strategic Goal 6: Build and Sustain a High-Quality OIG Work Environment	$2,493,000	10%	11	8%
Total	**$25,756,000**	**100%**	**130**	**100%**

APPENDIX III

External Factors

The following table briefly describes the external factors that could affect the achievement of the strategic and performance goals in this plan.

External Factor	Description
Budget	The OIG receives an annual appropriation from the Congress under Section 1105(a) of Title 31, United States Code. Our ability to accomplish our strategic and annual goals is dependent upon adequate funding through this appropriations process. The OIG will operate under a Continuing Resolution providing temporary funding for the initial part of FY 2007. Our planned work could be impacted by appropriation decisions that will be made later.
External Requests	Periodically, the OIG receives requests for work from members of Congress or FDIC officials. These requests may require greater priority than work we have planned for in our strategic and annual performance plan and could result in a reallocation of resources.
Number of Bank Failures	In the last few years, the economy has been strong and banks have prospered. The rate of bank and thrift failures has remained at a relatively low level over the past 10 years. In fact, 2005 was the first year in the FDIC's history where no institutions have failed, nor has 2006 seen any failures to date. However, business cycles can change and a large number of bank failures could increase the OIG's workload and result in the diversion of resources from planned activities to bank resolution activities.
Emerging Technology	Emerging technology has introduced new ways for banks to offer traditional products and services to their customers. With technological advancements, there is increased risk that fraud and other inappropriate activity may occur. A reallocation of OIG resources could be needed to ensure that such risks are appropriately addressed.
Changes in Financial Services Industry	Over the past 20 years, unprecedented changes have taken place in the financial services industry that have significantly changed and shaped the environment in which the FDIC and the other financial regulatory agencies operate. More major changes may be in store in the coming years. The OIG will monitor these and other emerging issues and risks as they develop to ensure they are appropriately addressed. This may require a reallocation of our resources and workload.

APPENDIX IV

Program Evaluations

The following table briefly describes the program evaluations, studies, and other assessments used to review and revise our strategic and performance goals.

	Description
Management and Performance Challenges	In the sprit of the Reports Consolidation Act, the OIG annually identifies the most significant management and performance challenges (MPCs) facing the Corporation. The OIG identified the following MPCs for 2006. ▪ 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; and ▪ Managing and protecting financial, human, information technology, and procurement resources.
Audit and Evaluation Assignment Plan	Describes audit and evaluation projects to be started during the year. The plan is linked to FDIC program goals and considers the OIG's identification of MPCs. Input is solicited from senior FDIC management and members of the FDIC Audit Committee.
Client Meetings	Meetings were held throughout FY 2006 with top management of FDIC divisions to discuss potential OIG work of strategic importance.
OIG Human Capital Strategic Plan	Identifies strategies for aligning human resources policies and procedures to support the OIG mission.
OIG Information Technology Strategic Plan	Sets forth challenges and strategies for the OIG's information technology needs for fiscal years 2005-2007.
Internal Quality Assurance Reviews	Reviews conducted by the OIG of our internal operations.
External Peer Reviews	Evaluation conducted of the OIG's audit operations by the Department of Energy OIG in 2003-2004.
Internal Control Reviews	Assessments of OIG accountability units conducted by the OIG under the Corporation's Internal Control and Risk Management Program.

APPENDIX V

Verification and Validation of Performance Data

The following table describes the sources for our performance data and how the data will be verified and validated.

Data Source	Description
System for Tracking Audits and Reports (STAR)	STAR tracks information on audit and evaluation assignments, reports, recommendations, time, and independent public accountant assignments, and provides managers with reports on those activities. STAR is used to generate performance measurement data reported in our annual performance reports as well as provide statistics for the OIG's Semiannual Report to the Congress. The data and related reports are analyzed by OIG staff for accuracy, reasonableness, and completeness. In addition, other controls such as edit checks and supervisory review of data input are used to ensure the validity and integrity of the performance data and reports.
Investigations Database System (IDS)	IDS was designed specifically, in part, to more accurately track the measures and goals we have established under the strategic and annual performance plans. The Web-based system tracks information on investigative cases opened and closed; fines, restitution, and other monetary recoveries; and judicial and administrative actions. We also have an inspection regimen set up to closely monitor the activities of our investigative offices and to ensure the accuracy of data entered into the database.
OIG Strategic Information Dashboard (Dashboard)	The Dashboard is an information system designed to improve the efficiency of OIG management oversight of internal operations. It provides OIG executives and staff with up-to-date information on the status of the OIG's annual performance goals and key efforts, quantitative performance measures and indicators, and budget and staffing data.

Appendix VI

FY 2007 Audit and Evaluation Assignments

This appendix presents a brief description of the audit and evaluation assignments that we plan to start in fiscal year 2007, including the assignment objective, background information, relevant prior coverage, known risks, and the estimated timeframes for starting and completing the work. The list of assignments is organized by the OIG's strategic goal so that stakeholders can clearly see how individual assignments support the OIG's business planning framework.

This listing reflects input we received from key stakeholders, including FDIC management and members of the Audit Committee, during the OIG's business planning process, as well as during other routine discussions that OIG representatives have had with FDIC officials. The dialogue with FDIC executives and managers together with the increased emphasis within our organization on planning is a critical part of our continuing efforts to identify those areas where the OIG can devote resources in the best interest of the Corporation and meet our responsibilities under the IG Act.

In addition to the list of assignments that we plan to start, a number of assignments started in Fiscal Year 2006 and will be completed during Fiscal Year 2007. We have included a list of those assignments on the last page of the Appendix. Our planning process is ongoing and dynamic, and we may alter the focus, timing, and selection of audits and evaluations to better respond to legislatively mandated priorities, congressional requests, emerging issues, FDIC corporate governance issues, and changing priorities within the FDIC.

Strategic Goal 1: Assist the FDIC to Ensure the Nation's Banks Operate Safely and Soundly

1. Material Loss Reviews (MLR) [AUDIT]

The OIG of the respective primary federal regulator is required by the FDIC Improvement Act of 1991 (FDICIA) to perform a material loss review (MLR) and report on failures of insured depository institutions resulting in losses to the deposit insurance funds which exceed the greater of $25 million or 2 percent of the institution's assets. MLRs must be completed within 6 months from the time it is determined that a failure or payment of financial assistance will result in a material loss to the insurance funds.

The audit objectives, as required by the FDICIA, section 38, are to determine (1) the causes for a material loss to a deposit insurance fund caused by an FDIC-supervised institution and (2) the adequacy of the FDIC's supervision of the institution, including implementation of Prompt Corrective Action requirements.

Projected Start **N/A**
Expected Report Issuance **N/A**

2. Examination Assessment of Interest Rate Risk [AUDIT]

Interest rate risk is fundamental to the business of banking. Changes in interest rates can expose an institution to adverse shifts in net interest income, increase the cost of funds, and impair the underlying value of its assets. Bank examiners assess the level of interest rate risk exposure in light of a bank's asset size, complexity, levels of capital and earnings, and most important, the effectiveness of its risk management processes. At the core of the interest rate risk examination process is a supervisory assessment of how well bank management identifies, monitors, manages, and controls interest rate risk. This assessment is summarized in an assigned risk rating for the component known as sensitivity to market risk, which is the "S" part of the CAMELS rating system. A June 2005 article in the FDIC's Supervisory Insights stated that rising interest rates and a flattening yield curve could pressure net interest margins, particularly for liability-sensitive banks with increased exposure to long-term assets. The article noted that it is difficult to draw conclusions about the level of interest rate risk based solely on off-site information. This assignment continues the series of OIG audits that have focused on individual CAMELS rating components.

The audit objectives are to (1) determine whether the FDIC's examinations comply with applicable policies and procedures for assessing and addressing institutions' sensitivity to interest rate changes and (2) evaluate how examiners consider off-site and industry-wide analysis in assessing interest rate risk.

Projected Start **3rd Quarter – FY 2007**
Expected Report Issuance **1st Quarter – FY 2008**

3. The FDIC's Oversight of Subprime Lending at FDIC-Supervised Institutions [AUDIT]

Subprime lending refers to programs that target borrowers with weakened credit histories typically characterized by payment delinquencies, previous charge-offs, judgments, or bankruptcies. Since the 1990s, subprime lending volumes have increased significantly and financial regulators, including the FDIC, have closely monitored and responded to that trend. In July 2001, Federal banking regulatory agencies jointly issued expanded examination guidance on subprime lending. In issuing the guidance, regulators recognized that subprime lending can expand credit access for consumers and offer institutions the opportunity to earn attractive returns. However, the risks associated with this activity must be properly controlled and managed to help ensure an institution's fundamental safety and soundness. The expanded guidance applies specifically to those institutions that have subprime lending programs with an aggregate credit exposure greater than or equal to 25 percent of tier 1 capital. Prior OIG audit work focused on the FDIC's process for assessing subprime lending using previously issued regulatory guidance and more recent work focused on predatory lending.

The audit objectives are to determine whether (1) the FDIC's institution and examiner guidance provides appropriate protection to consumers and helps ensure the safety and soundness of institutions, (2) examiners receive sufficient training related to subprime lending, and (3) examinations are conducted in accordance with subprime lending guidance.

Projected Start **1st Quarter – FY 2007**
Expected Report Issuance **3rd Quarter – FY 2007**

4. Technology Service Provider (TSP) Examinations for Independent Data Centers [AUDIT]

An increasing number of insured institutions are outsourcing software development and maintenance, data processing, and other information technology (IT) services to TSPs. In many cases, these outsourced services are critical to the institutions' daily operations and fall within the purview of bank examiners. Key components of the payments system, including credit card services and automated teller machine networks, are also operated and managed by TSPs. The Federal Financial Institutions Examination Council (FFIEC) has established a process for examining these companies. For TSPs that are owned or controlled by, or otherwise affiliated with, an FDIC-supervised financial institution, examination coverage is provided through the IT examination of the institution. The client base of major TSP firms has grown significantly during the past several years and the level of risk to financial institutions may correspondingly increase because any financial or operational problems these TSPs experience would affect a greater number of clients. Recent OIG audit work focused on assessing the FDIC's oversight process for identifying and monitoring TSPs used by FDIC-supervised institutions and prioritizing examination coverage, and IT examination coverage related to vendor management.

The audit objective is to assess the FDIC's implementation of the FFIEC and FDIC guidance for conducting examinations of independent data centers.

Projected Start **1st Quarter – FY 2007**
Expected Report Issuance **3rd Quarter – FY 2007**

5. Implementation of the USA PATRIOT Act [AUDIT]

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) (Public L. No. 107-560), enacted on October 26, 2001, was passed by the United States Congress in response to the September 11, 2001 attacks and made a number of amendments to the anti-money laundering provisions of the BSA. Title III: International Money Laundering Abatement and Financial Anti-Terrorism is intended to facilitate the prevention, detection, and prosecution of international money laundering and terrorist financing. Congress found that money laundering "provides the financial fuel that permits transnational criminal enterprises to conduct and expand their operations to the detriment of the safety and security of American citizens" and that it is critical to the financing of global terrorism and terrorist attacks. Accordingly, FDIC examiners play a critical role in ensuring that institutions comply with the Act.

The audit objectives are to determine whether (1) examination procedures are designed to evaluate institution compliance with anti-money laundering and terrorist financing provisions of the USA PATRIOT Act and (2) those procedures are fully and consistently implemented to provide reasonable assurance that institutions with weak programs for detecting money laundering and terrorist financing activity will be identified and appropriate corrective measures imposed.

Projected Start **1st Quarter – FY 2007**
Expected Report Issuance **3rd Quarter – FY 2007**

Strategic Goal 2: Help the FDIC Maintain the Viability of the Insurance Fund

6. Dedicated Examiner Program for Large Institutions [AUDIT]

The FDIC has reported that the increased complexity of the industry and the concentration of risk to the insurance funds in the largest banking organizations are expected to grow more pronounced over time and to present greater risk-management challenges to the Corporation. As insurer, the FDIC needs a comprehensive understanding of the risks that the largest institutions pose to the Deposit Insurance Fund. A primary objective of the Division of Supervision and Consumer Protection's (DSC) large insured depository institution program is to assess and quantify the risks posed by these large and complex institutions from a deposit insurer's perspective. The FDIC is not the primary federal regulator for most of the large institutions it insures. Therefore, the risk assessment process is based on a combination of information obtained from the primary federal regulator, the institution, supervisory activities,

market data, and publicly available data. The FDIC operates several programs to supervise and assess large bank risks. The FDIC established the Large Bank Branch in headquarters to coordinate the FDIC's nationwide programs focused on supervising and assessing risk in large institutions. One of the key large bank programs is the Dedicated Examiner Program which was established in 2002. This program established dedicated examiners in the six largest insured depository institutions to work in cooperation with primary supervisors and bank personnel to obtain real-time access to information about the risk and trends in those institutions. Prior audit work focused on the FDIC's special examination authority and efforts to monitor large bank risks before the dedicated examiner program was established.

The audit objective is to determine whether the Dedicated Examiner Program is working as envisioned, that is, allowing the FDIC access to information it needs to assess and quantify the risks posed by large institutions to the Deposit Insurance Fund.

Projected Start **1st Quarter – FY 2007**
Expected Report Issuance **3rd Quarter – FY 2007**

7. FDIC's Approach to Managing External Risks [EVALUATION]

The FDIC has an Office of Enterprise Risk Management (OERM) that focuses on the risks internal to the FDIC. External risk management is a primary responsibility of FDIC's Division of Insurance and Research, DSC, and Division of Resolutions and Receiverships (DRR). The FDIC has taken a series of steps over the last several years to better integrate its risk management process. In early 2003, the FDIC created the National Risk Committee (NRC), a cross-divisional body of senior managers established to identify and evaluate major business risks facing the banking industry and insurance fund. The NRC is supported by a network of regional risk committees. Additionally, the FDIC established the Risk Analysis Center in 2003 to monitor emerging macro and micro risks on a daily basis and recommend responses to the NRC. The third component to the FDIC's risk management structure is the Financial Risk Committee, whose broad mission is to quantify risks to the deposit insurance fund for financial reporting and fund management purposes. In 2003, the FDIC commissioned an independent study that focused on financial risk management in the FDIC. That review also included an assessment of the NRC and the Risk Analysis Center and made specific recommendations aimed at strengthening the FDIC's risk management processes over time.

The objective is to evaluate the extent to which the FDIC has established an enterprise risk management framework for identifying, assessing, and responding to risks facing the deposit insurance fund, including how the FDIC ensures that relevant information is identified, captured, and communicated.

Projected Start: **4th Quarter 2007**
Expected Report Issuance: **2nd Quarter 2008**

Strategic Goal 3: Assist the FDIC to Protect Consumer Rights and Ensure Data Security and Privacy

8. Examination Assessment of Offshore Outsourcing of Data Services [AUDIT]

Financial institutions have been outsourcing to domestic third-party service providers or domestic affiliates for many years. Offshoring is the performance of day-to-day activities from a remote location typically not in an organization's country of origin. The use of offshore contractors has grown dramatically in the past few years due to the flexibility offered by new technology and the prospect of lower costs. Domestic outsourcing and offshoring share many risk characteristics. However, the more complicated legal structure and chain of control incurred when offshoring financial services may create new risks when compared to domestic outsourcing. The FDIC assesses the risks related to offshoring as part of its IT examination process. Significant offshoring risk areas associated with data security include:

- Operations/Transactions Risk – weak controls may affect bank operations.
- Compliance Risk – offshore vendors may not have adequate privacy controls.

Prior audit work focused on FDIC's IT examination process more broadly.

The audit objective is to evaluate how the FDIC identifies offshore outsourcing activities in FDIC-supervised institutions and assesses the programs those institutions have in place to address the data security risks associated with offshore outsourcing.

Projected Start **1st Quarter – FY 2007**
Expected Report Issuance **3rd Quarter – FY 2007**

9. Compliance Management System [AUDIT]

The FDIC has supervisory responsibilities for ensuring that the financial institutions it supervises comply with fair lending, privacy, and various other consumer protection laws and regulations. The FDIC uses its compliance examination process to ascertain the effectiveness of an institution's program for complying with consumer protection laws and regulations. DSC compliance examinations 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. A financial institution must develop and maintain a sound compliance management system that is integrated into the overall risk management strategy of the institution. A compliance management system, which is comprised of board and management oversight, a compliance program and compliance audit, is how an institution: learns about its compliance responsibilities; ensures that employees understand these responsibilities; ensures that requirements are incorporated into business processes; reviews operations to ensure responsibilities are carried out and requirements are met; and takes corrective action and updates materials as necessary.

The audit objective is to determine whether DSC is adequately assessing financial institutions' compliance management systems during the compliance examination process.

Projected Start **3rd Quarter – FY 2007**
Expected Report Issuance **1st Quarter – FY 2008**

Strategic Goal 4: Help Ensure that the FDIC is Ready to Resolve Failed Banks and Effectively Manages Receiverships

10. DRR's Protection of Electronic Records [AUDIT]

Within the FDIC, DRR has the primary responsibility for resolving failed FDIC-insured depository institutions promptly, efficiently, and responsively to maintain public confidence in the nation's financial system. In performing their duties, DRR personnel have access to a wide variety of records containing personally identifiable information of the bank's employees and customers. These records may exist in hardcopy or electronic format. Given the increased risks associated with, and attention being placed on identity theft, the protection of customer information in the FDIC's systems is paramount to the FDIC's reputation. Prior OIG work focused on DRR efforts to protect personally identifiable information maintained in hardcopy form.

The audit objective is to evaluate the design and implementation of controls used by the FDIC to protect personal information collected and maintained in electronic form as a result of resolution and receivership activity.

Projected Start **3rd Quarter – FY 2007**
Expected Report Issuance **4th Quarter – FY 2007**

Strategic Goal 5: Promote Sound Governance and Effective Stewardship and Security of Human, Financial, IT, and Physical Resources

11. Records Management Program [EVALUATION]

Every Federal agency is legally required to manage its records. Records are the evidence of the agency's actions and support an agency's work to fulfill its mission. Therefore, records are a valuable resource and must be managed properly for the agency to function effectively and to comply with Federal laws and regulations. Records management addresses the life cycle of records, i.e., the period of time that records are in the custody of Federal agencies. The life cycle usually consists of three stages (1) creation or receipt, (2) maintenance and use, and (3) disposition. The FDIC has an established records management program, the goals of which are to:

- Protect the legal and financial rights of the Corporation and other entities directly affected by its activities.
- Ensure continuity and consistency in administration.
- Assist FDIC officials and their successors in making informed decisions.
- Provide the information required by Congress and others for overseeing the Corporation's activities.

Prior OIG work focused on safeguards over personal employee information, DRR efforts to protect personally identifiable information maintained in hardcopy form, and disposal of sensitive information by FDIC's records management contractor.

The objective is to evaluate FDIC's records management program to ensure that Corporation records are economically and efficiently managed to meet business needs and to comply with applicable laws and regulations. The evaluation may address: (1) to what extent the FDIC has a strategic approach to information management, (2) FDIC's records management program use of best practices, and (3) FDIC efforts to move to digital storage of Corporate records. This review could be scoped into multiple assignments.

Projected Start **3rd Quarter – FY 2007**
Expected Report Issuance **1st Quarter – FY 2008**

12. IT Project Management [AUDIT]

The Division of Information Technology (DIT) Project Management Office (PMO) was established in September 2005 as a resource center for clients, executives, project managers, and project team members engaged in the operations and oversight of IT projects. DIT initiated a PMO to establish standard repeatable project management practices and improve the results of IT project management activities. This PMO is organized to provide methodologies, oversight and expertise to support the successful completion of complex technology projects – the PMO does not provide direct management of individual projects. According to DIT's IT PMO policy, the PMO provides six key functions for FDIC's IT management community:

- Standards Management
- Monitoring
- Capacity Planning
- Portfolio Management
- Mentoring
- Governance

Prior audit work focused on IT capital management and FDIC's system development life cycle management before FDIC's PMO was established.

The objective is to assess FDIC's progress in improving project management and in keeping the decision-makers fully informed of the cost and status of major IT projects.

Projected Start **4th Quarter – FY 2007**
Expected Report Issuance **2nd Quarter – FY 2008**

13. Classifying Salary Costs in the NFE [EVALUATION]

The New Financial Environment (NFE) project was a major corporate initiative to enhance the FDIC's ability to meet current and future financial management and information needs. One of the organizational benefits NFE was designed to deliver is enhanced cost management. To that end, the cost management program was collaboratively created by all divisions and offices based on management's need for cost information. The cost management program is a framework of codes to which all costs are charged. The FDIC's cost management coding framework was implemented in May 2005. Costs are grouped into categories, called chartfields which are used to capture costs by business processes. The chartfields are used in NFE to capture the cost information. Approximately 70 percent of all the Corporation's costs are from salary (plus related benefits) and travel. The cost management program's success will rely on employees accurately entering all the necessary data into the appropriate cost management chartfields when reporting their time and travel.

The objective is to determine the extent to which salary costs are being appropriately classified in NFE and result in management information that is current, complete, accurate, and consistent to support management decision-making.

Projected Start **1st Quarter – FY 2007**
Expected Report Issuance **2nd Quarter – FY 2007**

14. Succession Planning Efforts [EVALUATION]

Federal agencies are faced with a growing number of employees who are eligible for retirement and are finding it difficult to fill certain mission-critical jobs— a situation that could significantly drain agencies' institutional knowledge. The Government Accountability Office (GAO) has reported that leading public organizations engage in broad, integrated succession planning and management efforts that focus on strengthening both current and future organizational capacity. The Corporation has reported that over the past 3 years it has focused considerable resources on human capital planning and is in the process of developing and implementing several key structural components of its human capital strategy for the future, including identification of succession planning and management strategies. Prior OIG evaluations have focused on other aspects of the FDIC's human capital program including its overall human capital framework, workforce planning, and the Corporate University.

The objective is to determine the extent to which the FDIC's succession planning efforts identify and address future critical staffing and leadership needs.

Projected Start **1st Quarter – FY 2007**
Expected Report Issuance **3rd Quarter – FY 2007**

15. FDIC's Career Program (Hiring Management) [EVALUATION]

In 2005, the FDIC established a new human capital framework and strategy to guide its planned evolution toward a more flexible permanent workforce that will be capable of responding rapidly to significant changes in the financial services industry or unexpected changes in workload or priorities. Over the past 12 years the Corporation was in a continuous downsizing mode as it completed the residual workload from the banking and thrift crises of the late 1980s and early 1990s but expects that significant downsizing activity is now complete. The FDIC is now working to pursue opportunities to begin reshaping its workforce to better align it with anticipated future human resource requirements. To facilitate this transition, the FDIC implemented a tool, FDIC Careers, Corporate Automated Recruiting, Evaluating, and Electronic Referral System, a fully automated hiring system in 2004, to make it easier for the FDIC to attract, screen and hire new employees. FDIC Careers is a new Web-based system that assists employees in finding and applying for jobs at the FDIC. FDIC Careers was developed by adapting a product known as "Quick Hire," owned by job-search Web site Monster.com, for use by the FDIC. With FDIC Careers, the Human Resources Branch works with managers to design specific questions to distinguish the best-qualified individuals. The system automatically quantifies the answers to those questions into a list of rated and ranked applicants.

The objective is to evaluate the efficiency, effectiveness, and customer satisfaction with FDIC's hiring program, procedures, and processes.

Projected Start **4th Quarter – FY 2007**
Expected Report Issuance **2nd Quarter – FY 2008**

16. Enterprise Architecture [AUDIT]

An Enterprise Architecture (EA) is a blueprint of an agency's current and planned operating and systems environment and the plan for transitioning between the two. Among other things, the EA defines principles and goals for, and sets direction on, IT security. The FDIC's framework for implementing its EA is based on federal and industry best practices, including the Chief Information Officer Council's Federal Enterprise Architecture Framework and the Zachman Framework for Enterprise Architecture. The seven components of the FDIC's EA framework include: Business, Information, Data, Applications, Technical Infrastructure, Security Architectures and E-Government Strategy. The FDIC is not legally required to develop an EA but recognizes its value and has decided to develop and implement an EA. The annual evaluation of FDIC's information security program covers the security aspect of EA and prior work has focused on FDIC's Capital Investment Management Review Process for IT Investments.

The audit objective is to assess the FDIC's progress in implementing an enterprise architecture program that supports the FDIC's mission.

Projected Start **2nd Quarter – FY 2007**
Expected Report Issuance **4th Quarter – FY 2007**

17. IT Risk Assessment [AUDIT]

The FDIC uses IT as a critical corporate resource in accomplishing its mission, goals, and objectives. From an internal perspective, the FDIC maintains a complex IT computing infrastructure that supports many business applications, processes sensitive information, and supports critical business operations. The FDIC recently completed a major transformation of its IT program that resulted in, among other things, the award of the largest IT contracts in the FDIC's history. From an external perspective, the FDIC assesses IT risks at FDIC-supervised institutions through industry outreach, regulation, and regular on-site IT examinations. GAO also conducts a review of the FDIC's IT controls as part of its annual audit of the FDIC's financial statements.

This assignment will leverage IT risk analysis work performed by the FDIC and consider the FDIC's complete IT environment (including IT management, technical infrastructure, applications, external connections, industry risks, etc.). The assignment will produce an IT risk analysis report that will be periodically updated and used to guide future IT audit assignments. The OIG has traditionally assessed corporate IT risks through ongoing audits, discussions with management, and monitoring of industry and regulatory issues. However, this approach will provide a more formal means for assessing IT risks facing the FDIC to help ensure that an appropriate level of audit attention is provided to the highest risk areas.

The objective is to complete a risk assessment of FDIC's IT environment, including corporate risk mitigation activities.

Projected Start **1st Quarter – FY 2007**
Expected Report Issuance **3rd Quarter – FY 2007**

18. The FDIC's Information Security Program--2007 [AUDIT]

On December 17, 2002, the President signed into law H.R. 2458, the E-Government Act of 2002 (Public Law 107-347). Title III of this act is the Federal Information Security Management Act (FISMA). FISMA directs federal agencies to have an annual independent evaluation performed of their information security programs and practices and to report the results of the evaluation to the Office of Management and Budget (OMB). FISMA states that the independent evaluation is to be performed by the agency Inspector General or an independent external auditor as determined by the Inspector General.

The audit objective is to evaluate the effectiveness of the FDIC's information security program and practices, including the FDIC's compliance with FISMA and related information security policies, procedures, standards, and guidelines. As part of our evaluation, we will assess the FDIC's efforts to improve its information security controls and practices relative to the baseline controls covered in our 2006 FISMA report and a new framework based on more recent government-wide guidance.

Projected Start **3rd Quarter – FY 2007**
Expected Report Issuance **4th Quarter – FY 2007**

19. IT Disaster Recovery Capability [AUDIT]

OMB policy requires agencies to establish and periodically test their ability to recover from IT service interruptions and to provide service based upon the needs and priorities of system participants. The FDIC conducts semiannual IT disaster recovery testing to ensure the Corporation's ability to recover its mainframe, midrange, and server platforms that would be required to restore IT operations in the event of a disaster. The FDIC has designated certain of its applications as "mission-critical" and includes these applications in its IT disaster recovery testing. The FDIC depends on the continuity of its IT operations to meet its business needs, financial obligations, and regulatory requirements. DIT conducted a semiannual IT disaster recovery test in April 2005 and experienced difficulties during the testing, including servers and critical applications that could not be recovered or tested and test scripts that did not execute as planned. DIT plans to relocate its IT disaster recovery capability to Richmond, Virginia. Our audit will evaluate the FDIC's IT disaster recovery capability following the planned move to Richmond. Prior work was completed in 2004 before the establishment of the facility in Richmond.

The audit objective is to determine whether the FDIC has established and implemented an IT disaster recovery capability that is consistent with federal standards, guidelines, and industry-accepted practices.

Projected Start **2nd Quarter – FY 2007**
Expected Report Issuance **4th Quarter – FY 2007**

20. Business Continuity Planning [AUDIT]

Recent large-scale disasters in the United States have clearly demonstrated how important it is to have reliable emergency response procedures and a well-written business continuity plan (BCP) to sustain critical business functions during an emergency or situation that may disrupt normal operations. The FDIC has developed an emergency operations program comprised of Emergency Response Plans and BCP. It is important, both symbolically and functionally, for federal government agencies to continue to serve the American public during any emergency or situation that may disrupt normal operations. We recently completed a review of FDIC's Emergency Response Plan, which coupled with this assignment, will complete planned follow–up work of a 2004 evaluation related to FDIC's business continuity planning. In 2003, we also completed an audit of the business continuity planning at FDIC-supervised institutions.

The objective to evaluate the extent of the FDIC's progress in developing and implementing comprehensive business continuity planning.

Projected Start **1st Quarter – FY 2007**
Expected Report Issuance **2nd Quarter – FY 2007**

21. Contract Rationalization [EVALUATION]

The OIG's report entitled, *Contract Administration*, stated that the FDIC currently does not have an effective information system for managing contracts. Historically, the Acquisition Services Branch maintained information about open and closed contracts using two different systems that were replaced when FDIC implemented NFE. Although NFE integrates financial and procurement information to some extent, the Acquisition Services Branch identified a number of gaps between current procurement business processes and NFE system capabilities. The Corporation has contracted with Oracle, Inc. to identify how best to use NFE and to suggest other system solutions for managing contracts. In the meanwhile, the FDIC better information on its existing inventory of contracts.

The objective is to assess whether FDIC has mechanisms in place to periodically evaluate the continuing need for contracts and determine whether there are corporate contracts that can be eliminated.

Projected Start **1st Quarter – FY 2007**
Expected Report Issuance **3rd Quarter – FY 2007**

22. Information Technology Application Services Task Order Awards [EVALUATION]

The FDIC, through the General Services Administration's FedBizOpps Electronic Posting System, solicited and selected several contractors to perform a wide range of IT services. The Information Technology Application Services contract combined approximately 40 contracts into 1 contract with multiple vendors for a total program value of $555 million over 10 years. In such a large contractual undertaking, significant risk may exist in getting the work completed and in overseeing the large task orders. Further, the actual task order award methodology and the level of detail in the descriptions of work are key to the FDIC avoiding protests and receiving needed goods and services at fair and reasonable prices.

The objectives are to determine whether the Information Technology Application Services contracting approach (1) is achieving anticipated benefits and (2) has an appropriate balance between controls in place and inherent risks.

Projected Start **1st Quarter – FY 2007**
Expected Report Issuance **2nd Quarter – FY 2007**

23. Contractor Reviews [EVALUATION]

The program of contractor reviews includes pre-award reviews of the FDIC's compliance with its contract evaluation and award process, pre-award reviews of contractor proposals or internal control systems, and contractor billing reviews. These assignments can result in monetary benefits, including recoveries of funds by the FDIC. In addition, the completion of a series of these assignments may identify common underlying problems resulting in opportunities to improve the contract solicitation, award, oversight, handling of claims, and closeout processes.

The audit objectives will vary by assignment type and include one or more of the following:

The objective of pre-award reviews is to (1) determine whether the FDIC is complying with its Acquisition Policy Manual in evaluating proposals and/or (2) assess financial aspects of bidders' proposals, including determining whether proposed costs are fair, reasonable, and supported.

The objective of billing reviews is to determine whether contractor billings are allowable under the contract, allocable, and reasonable.

Projected Start **4th Quarter – FY 2007**
Expected Report Issuance **4th Quarter – FY 2007**

24. FDIC's Enterprise Risk Management Program [EVALUATION]

OMB Circular A-123, Management's Responsibility for Internal Control, defines management's responsibility for internal control in federal agencies. The circular was revised in December 2004 to provide updated internal control standards and new specific requirements for conducting management's assessment of the effectiveness of internal control over financial reporting. The revision to the circular became effective in fiscal year 2006. Management is responsible for developing and maintaining effective internal control. Internal control guarantees neither the success of agency programs, nor the absence of waste, fraud, and mismanagement, but it is a means of managing the risk associated with programs and operations. OMB Circular A-123 states that federal managers must carefully consider the appropriate balance between controls and risk in their programs and operations. OERM is the corporate oversight manager for internal controls and risk management. OERM is working in partnership with all FDIC divisions and offices, helping them to identify, evaluate, monitor, and manage their risks.

The evaluation objective is to determine the extent to which the FDIC has implemented its Enterprise Risk Management Program consistent with applicable government-wide guidance and best practices.

Projected Start **1st Quarter – FY 2007**
Expected Report Issuance **3rd Quarter – FY 2007**

List of FY 2006 Carry-Over Assignments

1.	DSC's Oversight of Financial Institution Office Foreign Assets Control Compliance Programs **[AUDIT]**
2.	Audit of the FDIC's Procedures for Addressing IT Security of Supervised Banks **[AUDIT]**
3.	Interagency Agreement with GSA Under the FEDSIM Contract **[AUDIT]**
4.	Compliance with Section 522 of the Consolidated Appropriations Act of 2005 **[AUDIT]**
5.	FISMA Fiscal Year 2006 Management Report **[AUDIT]**
6.	Information Technology Examination Coverage of Vendor Management **[AUDIT]**
7.	Examination Assessment of Appraisals and Insurance **[AUDIT]**
8.	Effect of New Community Reinvestment Act Regulations **[AUDIT]**
9.	FDIC's Use of Performance Measures **[EVALUATION]**

Appendix VII

Internal Operational Improvement Projects

This appendix presents a brief description of our infrastructure or operational improvement projects, including estimated timeframes for starting and completing the work, under our internal Strategic Goal 6, Build and Sustain a High-Quality OIG Work Environment. The infrastructure projects cover a number of areas including professional development; human capital management and leadership development; client, stakeholder, and staff relationships; quality and efficiency of OIG work; strategic and annual performance planning and measurement; and information technology.

Professional Development

1. Develop a training and development plan for auditors, evaluators, and investigators.

The objective of this key effort is to create training and development plans that systematically target the developmental training needs of OIG auditors, evaluators, and investigators. The plans will provide a roadmap of curriculum and developmental experiences that auditors, evaluators, and investigators will use to systematically increase their job skills (including acquiring approved professional certifications), organizational knowledge, and leadership potential.

Projected Start: **1st Quarter – FY 2007**
Projected Completion: **3rd Quarter – FY 2007**

2. Explore expanding the pilot internal mentoring program.

The objective of this key effort is to review the OIG's pilot mentoring program and examine options for expanding it within the OIG. Three OIG employees and three mentors are participating in the pilot. Initially, we plan to collect feedback from the pilot participants regarding their experience and suggested improvements. We will also consider ways to expand the program and encourage further OIG participation.

Projected Start: **1st Quarter – FY 2007**
Projected Completion: **2nd Quarter – FY 2007**

Human Capital Management and Leadership Development

3. Include leadership development as a component of the auditor, evaluator, and investigator training plans.

The objective of this key effort is to create a training and development plan that systematically targets the developmental training needs of OIG staff. The plans will provide suggested curriculum and developmental experiences to systematically develop effective OIG leaders that can create a high performance environment, enhance succession planning, and result in a stronger leadership team.

Projected Start: **1st Quarter – FY 2007**
Projected Completion: **3rd Quarter – FY 2007**

4. Develop a pilot effort for end of assignment performance reviews.

The objective of this key effort is to develop and pilot a process for providing feedback at the end of each employee's assignment or after significant portions of work have been completed during the annual performance cycle. We aim to have the process ready for implementation on a pilot basis in the Office of Audits during the 2007 performance cycle. Our aim is to provide OIG staff with specific and timely performance feedback throughout the performance cycle and address both strengths and weaknesses.

Projected Start: **1st Quarter – FY 2007**
Projected Completion: **2nd Quarter – FY 2007** [with use and modification throughout 2007]

5. Award a contract for supplemental expertise for audits, evaluations, investigations, and other OIG activities.

The objective of this key effort is to have a multi-year contract in place that will allow the OIG to bring in a wide variety of experts and specialists on an as-needed basis to provide assistance and support on audits, evaluations, investigations, and other office activities. Work under the contract shall be authorized by issuance of task orders that will specify the nature, scope, and timing of the work to be performed by the contractor. The potential outcomes and benefits from this key effort include enhanced expertise on OIG audits, investigations, and projects.

Projected Start: **1st Quarter – FY 2007**
Projected Completion: **2nd Quarter – FY 2007**

6. Update business continuity and emergency preparedness plan.

The objective of this key effort is to monitor and update emergency preparedness in OIG to ensure the safety and security of personnel and the efficient resumption of our critical business processes in event of an emergency. We will monitor and update the OIG Business Continuity Plan to ensure restoration and resumption of key business functions within 30 days of an emergency and will monitor business continuity planning at field offices. This effort also includes an update and refinement of OIG emergency response planning to better ensure the safety and security of personnel during an emergency. We plan to feature pertinent aspects of emergency preparedness on the OIG Intranet.

Projected Start: **1st Quarter – FY 2007**
Projected Completion: **3rd Quarter – FY 2007**

7. Update workforce baseline data to aid in strategic human capital decision-making.

The objective of this key effort is to provide management with various workforce analyses to assist in strategic workforce planning. Analyses will include detailed information on number and composition of OIG staff, retirement eligibility of OIG staff,

and other information as requested. The analyses will lead to an improved ability to anticipate workforce needs and develop strategies for meeting those needs.

Projected Start: **2nd Quarter – FY 2007**
Projected Completion: **3rd Quarter – FY 2007**

Client, Stakeholder, and Staff Relationships

8. Complete and coordinate FDIC OIG congressional communications protocols.

The objective of this key effort is to issue in final a fully coordinated set of FDIC OIG congressional communication protocols. The protocols will serve as general principles governing the OIG's relations with the Congress and commitments to FDIC management. On October 31, 2005, the OIG issued the "FDIC OIG Congressional Communication Protocols" on an interim basis in anticipation of seeking FDIC management and congressional staff input at a later time. For this key effort, we would be affirming the protocols within the OIG and incorporating input from the OIG's clients and stakeholders.

Projected Start: **2nd Quarter – FY 2007**
Projected Completion: **3rd Quarter – FY 2007**

9. Elect new members to the Employee Advisory Group (EAG).

The mission of the Inspector General's Employee Advisory Group (EAG) is to provide employees of the OIG in non-managerial positions with the opportunity to provide information and feedback to the Inspector General on the overall working environment and business processes of the OIG. Its principal purpose is to help facilitate upward communication to the Inspector General. To do so, it will solicit employee opinions, present issues and suggestions raised by the staff to the Inspector General, propose solutions to issues when warranted, and act as a sounding board for the Inspector General. Write-ups of the EAG's activities will be posted to the OIG's Intranet site.

In light of reorganizations and downsizing of the OIG over the past several years, the EAG will re-examine its original charter and in consultation with the Inspector General will determine the optimum composition of the group and scheduling of meetings in order to accomplish its mission. Elections will be held and a new EAG will be in place by January 2007.

Projected Start: **1st Quarter – FY 2007**
Projected Completion: **1st Quarter – FY 2007**

Quality and Efficiency of OIG Work

10. Strengthen OIG audit assignment management controls.

The objective of this key effort is to strengthen assignment management controls and documentation of key audit decisions in assignment work papers. Tasks to be accomplished include reviewing the existing assignment management control framework and evaluating the extent that assignment management activities are effective and efficient and being or could be better documented in the assignment work papers. This analysis will be reviewed with the Inspector General to identify ways to improve the assignment management process and documentation of key engagement decisions. Necessary changes to the assignment management process and policies will be made.

Projected Start: **3rd Quarter – FY 2007**
Projected Completion: **1st Quarter – FY 2008**

11. Strengthen OIG audit policy and procedures.

The objective of this key effort is to update the Office of Audits policies and procedures manual to make any changes necessary as a result of revisions to *Government Auditing Standards*. The Government Accountability Office (GAO) is planning to issue revised standards in December 2006. The proposed 2006 changes to the standards include an increased emphasis on audit quality and ethics and an extensive update of the performance audit standards to include a specified level of assurance within the context of risk and materiality. GAO has proposed the standards become effective for performance audits beginning on or after July 1, 2007.

Projected Start: **1st Quarter – FY 2007**
Projected Completion: **3rd Quarter – FY 2007**

12. Host an external peer review of the OIG Office of Audits and resolve significant matters identified.

The objective of this key effort is to ensure that the external peer review team is readily provided access to and the information it needs to conduct the peer review of the Office of Audits (OA) and that appropriate action is taken to address any issues identified by the peer review team. The external peer review team will be determining whether OA's internal quality control system is adequate and complied with to provide reasonable assurance that applicable auditing standards, policies, and procedures are met. *Government Auditing Standards* require auditing organizations to undergo an external peer review at least once every 3 years. In the Inspector General community, the peer review is conducted using standards and guidelines published by the President's Council on Integrity and Efficiency. OA's last peer review was conducted by the Department of Energy OIG and reviewed the system of quality control of the year ended March 31, 2004. The report was issued September 1, 2004. The scope of an external review typically consists of the period of time covered by the two most recent Semiannual

Reports to the Congress, but may be expanded as deemed necessary by the review team. The Department of State OIG is scheduled to conduct a peer review of OA's 2006-2007 cycle meaning the review will cover OA's system of quality control for the year ended March 31, 2007. The Department of State OIG must issue its report by December 1, 2007, without requesting an extension from GAO.

Projected Start: **2nd Quarter – FY 2007**
Projected Completion: **4th Quarter – FY 2007**

13. Develop a project management tracking and reporting process for internal OIG projects.

The objective of this key effort is to develop a process for tracking and reporting on the milestones and progress related to the internal operational improvement projects and other projects in the OIG FY 2007 Business Plan. The process will provide a means for OIG management to assess whether key milestone dates are being met and projects are on schedule to be completed as planned.

Projected Start: **1st Quarter – FY 2007**
Projected Completion: **1st Quarter – FY 2007**

Strategic and Annual Performance Planning and Measurement

14. Continue with an outcome-oriented strategic and annual plan with performance targets for the OIG for FY 2008.

The objective of this key effort is to develop a FY 2008 Business Plan using approaches that were used in FY 2007 and to make changes desired by the Inspector General. We will also review our past practices to determine what changes can be made to enhance the business planning process.

Projected Start: **2nd Quarter – FY 2007**
Projected Completion: **4th Quarter – FY 2007**

Information Technology

15. Update the OIG IT Strategic Plan to guide OIG business decisions, priorities, and resource allocations for 2008-2010.

The objective of this key effort is to ensure that the investment and allocation of OIG information technology (IT) resources are well planned, justified, and appropriately aligned with and support the strategic goals of the OIG, as well as to ensure that they are managed effectively throughout their lifecycle.

Projected Start: **3rd Quarter – FY 2007**
Projected Completion: **4th Quarter – FY 2007**

16. Invest in modern laptop computers with enhanced security.

The objective of this key effort is to ensure that OIG laptop computers replaced during 2007 meet OIG operational, budgetary, and security requirements. OIG staff will participate with and coordinate activities with the Division of Information Technology related to evaluating, testing, and installing new laptop computers and related equipment. Particular attention will be given to safeguarding OIG data during the transfer to the new laptops.

Projected Start: **2nd Quarter – FY 2007**
Projected Completion: **3rd Quarter – FY 2007**

17. Review audit and evaluation information system options and requirements for efficiency and security.

The objective of this key effort is to identify and evaluate the options and requirements needed to streamline, enhance, and improve the collection and reporting of information needed to manage OIG audits and evaluations. Current information systems and automated tools will be evaluated and analyzed according to OIG management's information requirements to determine an optimal approach to meeting those requirements in a cost-effective and timely manner. A particular focus is on minimizing data entry, providing graphical representations of information, improving performance, and providing information across OIG systems and applications.

Projected Start: **2nd Quarter – FY 2007**
Projected Completion: **2nd Quarter – FY 2007**

18. Update OIG training system to be more efficient monitoring continuing professional education requirements.

The objective of this key effort is to streamline and improve Training System processes for submitting, reviewing, approving, reporting, and monitoring training requests to ensure the continuing professional education hours earned by OIG staff meet current GAO Government Auditing Standards for continuing professional education requirements. This is a major upgrade to the Training System that focuses on providing Office of Audits and Office of Evaluations staff and management with significant improvements in submitting, reviewing, approving, and reporting training requests that provide CPE hours. In addition, the system is being upgraded to streamline and improve several other key features including security, data entry, payment processing, and administrative activities.

Projected Start: **4th Quarter – FY 2006**
Projected Completion: **1st Quarter – FY 2007**

19. Update the Dashboard to incorporate FY 2007 Business Plan goals and key efforts.

The objective of this key effort is to reset the Dashboard to provide reporting on the status of FY 2007 qualitative and quantitative performance goals and measures. In addition, part of this effort will involve archiving FY 2006 performance results. The completion of this key effort will enhance our ability to update and report out on our FY 2007 performance goals and key efforts.

Projected Start: **1st Quarter – FY 2007**
Projected Completion: **1st Quarter – FY 2007**

Appendix VIII

Other Projects

20. Operate a Suspicious Activity Report (SAR) database and participate in other law enforcement/regulatory task groups formed to review SARs.

The objective of this project is to enhance the OIG's Office of Investigations and the Division of Supervision and Consumer Protection's ability to identify, analyze, and address fraud cases impacting the FDIC.

Projected Start: **Ongoing**
Projected Completion: **1st Quarter FY 2007**

21. Respond to any bank closing where fraud is suspected to have played a role in the failure of the institution.

The objective of this project is to foster a strong partnership between the OIG's Office of Investigations, the Division of Resolutions and Receiverships (DRR), and the Legal Division by providing support through advice and expertise in the detection, investigation, and the collection of electronic evidence relating to complex financial and computer-related frauds at bank closings. An investigative team, to include Electronic Crimes Unit agents, will respond in the event of such a closing, and will share data imaged from the closing, as needed, with the FDIC.

Projected Start: **Ongoing**
Projected Completion: **3rd Quarter FY 2007**

22. Monitor DRR's planning for a potential large bank failure.

One of the greatest risks to the Deposit Insurance Fund and public confidence in the nation's financial system would be the failure of a large American bank. Such a failure could overwhelm the resources of the FDIC and could cause a public panic. The FDIC is putting plans in place to deal with a significant bank failure. The OIG will be monitoring the development of the plans and will participate in any simulation exercise. The OIG must be ready for a large bank failure where fraud is a contributing factor. In addition, the OIG must be ready to review the circumstances that cause a large bank failure and make recommendations, if appropriate, to strengthen the regulatory process.

Projected Start: **1st Quarter FY 2007**
Projected Completion: **4th Quarter FY 2007**

23. Host the Emerging Issues in Banking Symposium.

The FDIC OIG, along with the Federal Reserve Board, Department of the Treasury, and National Credit Union Administration OIGs will cosponsor an *Emerging Issues in Banking Symposium*. This symposium provides a forum for representatives from the financial regulatory agency Offices of Inspector General, Government Accountability Office, Securities and Exchange Commission, Pension Benefit Guaranty Corporation, Federal Housing Finance Board, and others to hear from leading experts and Congressional representatives about emerging issues that impact our collective and individual work and responsibilities. The FDIC OIG will coordinate the symposium with the other financial regulatory OIGs and will plan to host the forum at the Virginia Square site.

Projected Start: **2nd Quarter FY 2007**
Projected Completion: **1st Quarter FY 2008**

24. Support PCIE activities.

The President's Council on Integrity and Efficiency (PCIE) was established by Executive Order on May 11, 1992 to address integrity, economy, and effectiveness issues that transcend individual government agencies, and increase the professionalism and effectiveness of OIG personnel throughout the government. It is principally comprised of the Presidentially appointed IGs. The FDIC OIG will participate fully in the activities of the PCIE, including attending monthly meetings, sharing information and best practices, partnering with other OIGs on cross-cutting projects of mutual interest, conducting peer reviews, supporting PCIE-sponsored training and professional development programs, and responding to various data calls throughout the year. The Inspector General is the principal participant in PCIE activities. The Deputy Inspector General and other members of the OIG's executive management team and the PCIE Liaison support the Inspector General's involvement in PCIE matters.

Projected Start: **Ongoing**
Projected Completion: **4th Quarter FY 2007**

25. Hold OIG Conference 2007.

The OIG will hold an officewide conference during the week of April 16-20, 2007. A major focus of the conference will be the progress of many of the key efforts and infrastructure improvement initiatives contained in the 2007 Business Plan. The Office of Investigations will use part of the week to conduct its required legal training. Other component offices of the OIG may elect to plan individual business meetings or training during the same week.

Projected Start: **1st Quarter FY 2007**
Projected Completion: **3rd Quarter FY 2007**

26. Communicate with corporate stakeholders.

The FDIC OIG is committed to establishing and maintaining effective working relationships with others in the Corporation. To ensure a full understanding of the role and activities of the OIG, the Inspector General and other OIG Executives will meet regularly with FDIC senior management and report back to others in the OIG on the results of those meetings. The OIG will also continue to participate in corporate-sponsored forums and meetings. We will keep track of meetings and commitments made by the OIG and the OIG's participation in corporate events; inventory the timing and content of current coordination and communication efforts and explore ways to improve on those; develop new brochures, briefing materials, presentations, and other products to communicate the mission of the OIG and its component offices; and pursue additional opportunities to sustain solid working relationships with corporate officials.

Projected Start: **1st Quarter FY 2007**
Projected Completion: **3rd Quarter FY 2007**

27. Enhance industry outreach.

The OIG plans to broaden its outreach efforts to the banking community. Given our experience and expertise auditing and evaluating FDIC programs and operations and investigating financial institution fraud, we have valuable insights and perspectives to share with the banking industry. We will review our current industry outreach strategies and seek to expand opportunities to attend and make presentations at meetings, conferences, and other such forums as we work to assist and augment the FDIC's contribution to stability and public confidence in the Nation's banking system.

Projected Start: **1st Quarter FY 2007**
Projected Completion: **2nd Quarter FY 2007**

28. Conduct an external peer review of the Department of Justice OIG audit function.

The objective of this key effort is to conduct an external peer review to determine whether the reviewed audit organization's internal quality control system is adequate and complied with to provide reasonable assurance that applicable auditing standards, policies, and procedures were met. *Government Auditing Standards* require auditing organizations to undergo an external peer review at least once every 3 years. In the Inspector General community, the peer review is conducted using standards and guidelines published by the President's Council on Integrity and Efficiency. The FDIC OIG's Office of Audits is responsible for completing a peer review of the Department of Justice OIG Office of Audits. OA must issue the report by June 3, 2007, without requesting an extension from the Government Accountability Office. An entrance conference was held September 6, 2006, and OA plans to complete the review and issue the final report in February 2007.

Projected Start: **4th Quarter – FY 2006**
Projected Completion: **2nd Quarter – FY 2007**


Office of Inspector General
2007 Business Plan
Other
Projects
Operational
Improvement
The Office of Inspector General's
Strategic Plan and
FY 2007 Performance Plan
Federal Deposit Insurance Corporation
November 2006