

# Office of Inspector General 2006 Business Plan



The Office of Inspector General's  
Strategic Plan and  
FY 2006 Performance Plan





# Inspector General Foreword

February 2006

I am pleased to present the Business Plan for the Office of Inspector General (OIG) at the Federal Deposit Insurance Corporation (FDIC). This plan combines the Strategic Plan for fiscal years 2006 through 2011 and Performance Plan for fiscal year 2006. The plan represents the results of concerted efforts over time, and especially during the past year, to improve our planning process and further increase the value added by our office to sound FDIC governance and to executive and legislative branch decision-makers.



Since the Great Depression, the FDIC has been and continues to be a pillar of America's stable and prosperous financial system. Our work and efforts are aimed toward maintaining and enhancing the FDIC's contributions to the nation's prosperity. The OIG has a unique role, mandated by statute, to be an independent and objective oversight unit within the FDIC. While the inherent nature of our

role sometimes causes a natural tension with other agency officials, we remain committed to being a valuable contributor to the Corporation.

Effectively conveying to all our stakeholders, including all OIG employees, what we are about, what we want to accomplish, how we will get there, and how our results can be evaluated is critical for our success. This Business Plan communicates those factors. We will strive to

demonstrate to the Congress, the public, the FDIC, and the banking industry that the OIG is doing the right things and generating results that are a worthy return on the investment made in us. Our work this year and years after will be the measure of our success.

Patricia M. Black  
Deputy Inspector General



---

# Table of Contents

Inspector General Foreword .....	1
Mission, Goals, Means, and Strategies .....	3
Business Plan Framework.....	7
Strategic Goal 1: Assist the FDIC to Ensure the Nation’s Banks Operate Safely and Soundly .....	8
Strategic Goal 2: Help the FDIC Maintain the Viability of the Insurance Funds.....	13
Strategic Goal 3: Assist the FDIC to Protect Consumer Rights and Ensure Community Reinvestment .....	16
Strategic Goal 4: Help Ensure that the FDIC is Ready to Resolve Failed Banks and Effectively Manages Receiverships.....	21
Strategic Goal 5: Promote Sound Governance and Effective Stewardship of Financial, Human, IT, and Procurement Resources .....	25
Strategic Goal 6: Continuously Enhance the OIG’s Business and Management Processes.....	35
Quantitative Performance Measures and Targets .....	42
Appendices	
I.    OIG Organization Structure.....	43
II.   Resource Allocation by Strategic Goal.....	45
III.  External Factors .....	46
IV.  Program Evaluations.....	47
V.   Verification and Validation of Performance Data .....	48





# Mission, 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 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 that we seek to add value to the Corporation and be one of the best OIGs in government.

---

## *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 considered the FDIC's strategic goals and the Chairman's 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:

- Assist the FDIC to ensure the nation's banks operate safely and soundly
- Help the FDIC maintain the viability of the insurance funds
- Assist the FDIC to protect consumer rights and ensure community reinvestment
- Help ensure that the FDIC is ready to resolve failed banks and effectively manages receiverships

- Promote sound governance and effective stewardship of financial, human, information technology, and procurement resources

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

- Continuously enhance the OIG's business and management processes.

### **Performance Measures**

Past OIG strategic and performance plans sought to define our goals and measure performance in almost exclusively quantifiable terms. In updating our plan, we revised our focus to include performance measures more reflective of mission-related goals and outcomes. We have added qualitative performance goals to complement our quantitative performance measures. Each qualitative performance goal includes a set of key efforts representing ongoing work or work to be undertaken during 2006 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.

Our quantitative measures have been streamlined to a few key measures with a greater emphasis on outcomes and results. These measures include financial benefits resulting from our audits 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. A complete list of our quantitative measures, along with our targets for FY 2006, is shown in the table on page 42.

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.

---

### ***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 assignment plans, which outline planned audit and evaluation coverage for the coming year, are 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 audit assignment plans, 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/or Vice Chairman through briefings about ongoing and completed work and is a regular participant on the Audit Committee. The OIG also places a high priority on building strong alliances with the U.S. Government Accountability Office, 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 80 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 which have resulted in bank consolidations and improved financial health and to 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 the target staffing level of 133 in fiscal year 2006. During the period, our Office of Audits has been reduced about 50 percent. These changes have profound implications on the work that can be accomplished and is reflected in some lowered performance targets discussed later in the Business Plan.

### **Information Technology**

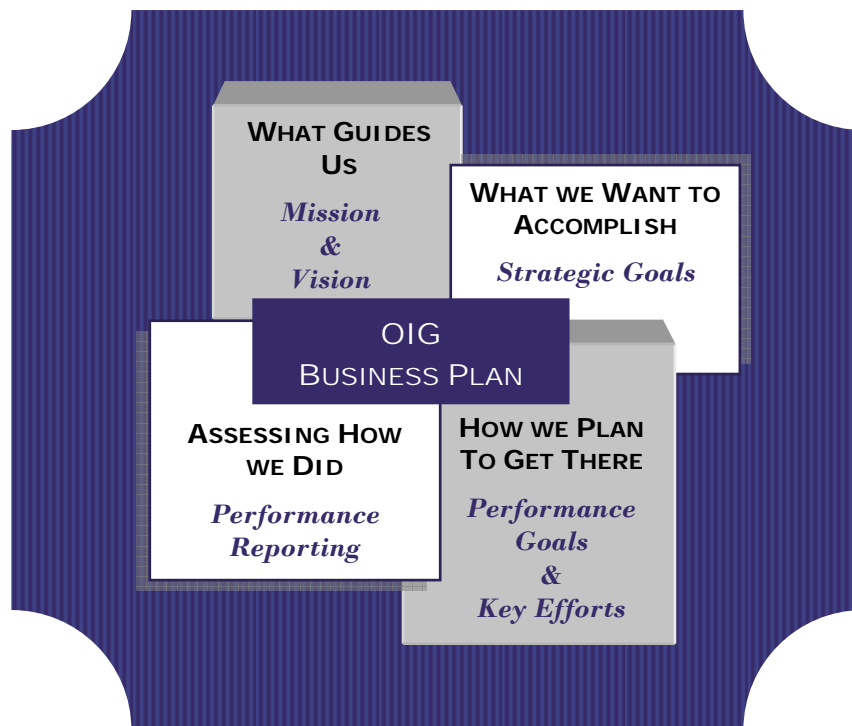
Our information technology (IT) goal is to better link IT planning and investment decisions to our mission and goals, thus helping ensure that OIG managers and staff have the IT tools and services they require to successfully and productively perform their work. The OIG IT vision is to enable our managers 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. 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 and conflict 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 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

### (2006 – 2011)

#### **VISION**

*We seek to add value to the Corporation and be one of the best OIGs in government.*

#### **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**

<u>Supervision</u>	<u>Insurance</u>	<u>Consumer Protection</u>	<u>Receivership Management</u>	<u>FDIC Resources Management</u>	<u>OIG Internal Processes</u>
Assist the FDIC to ensure the nation's banks operate safely and soundly	Help the FDIC maintain the viability of the insurance funds	Assist the FDIC to protect consumer rights and ensure community reinvestment	Help ensure that the FDIC is ready to resolve failed banks and effectively manages receiverships	Promote sound governance and effective stewardship of financial, human, IT, and procurement resources	Continuously enhance the OIG's business and management processes

#### **FY 2006 PERFORMANCE GOALS**

<ul style="list-style-type: none"> <li>▪ Ensure the effectiveness of the FDIC's supervision program</li> <li>▪ Assist efforts to detect and prevent bank secrecy violations, fraud, and financial crimes in FDIC-insured institutions</li> </ul>	<ul style="list-style-type: none"> <li>▪ Evaluate corporate programs to identify and manage risks in the banking industry that can cause losses to the funds</li> <li>▪ Assess the management of the deposit insurance funds</li> </ul>	<ul style="list-style-type: none"> <li>▪ Evaluate the effectiveness of FDIC programs for protecting consumer privacy</li> <li>▪ Review fair lending and community reinvestment examination programs</li> <li>▪ Strengthen enforcement against misrepresentations of deposit insurance coverage</li> </ul>	<ul style="list-style-type: none"> <li>▪ Evaluate the FDIC's plans and systems for managing bank failures</li> <li>▪ Assist the FDIC in recovering financial losses from individuals fraudulently concealing assets</li> </ul>	<ul style="list-style-type: none"> <li>▪ Evaluate corporate efforts to fund operations efficiently, effectively, economically</li> <li>▪ Assess human capital strategic initiatives</li> <li>▪ Promote a high return on resource investments and ensure IT and physical security</li> <li>▪ Evaluate corporate contracting efforts</li> <li>▪ Monitor corporate risk management and internal control efforts</li> </ul>	<ul style="list-style-type: none"> <li>▪ Enhance strategic and annual planning and performance measurement</li> <li>▪ Strengthen human capital management</li> <li>▪ Ensure quality and efficiency of OIG audits, evaluations, &amp; investigations</li> <li>▪ Foster good client, stakeholder, &amp; staff relationships</li> <li>▪ Invest in cost-effective, secure IT</li> </ul>
--	---	---	--	---	---



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

Bank supervision is a cornerstone of the FDIC's efforts to ensure stability and public confidence in the nation's financial system. As of September 30, 2005, the FDIC was the primary federal regulator for 5,245 FDIC-insured, state-chartered institutions that were not members of the Federal Reserve System (generally referred to as "state non-member" institutions). Other banks and thrifts are supervised by the Department of the Treasury (the Office of the Comptroller of the Currency and the Office of Thrift Supervision) or the Federal Reserve Board depending on the institution's charter. While the number of institutions where the FDIC is the primary federal supervisor showed a steady decline over the past four years, the dollar value of assets held by those institutions showed a steady increase during the same period as, depicted in Figure 1.1.

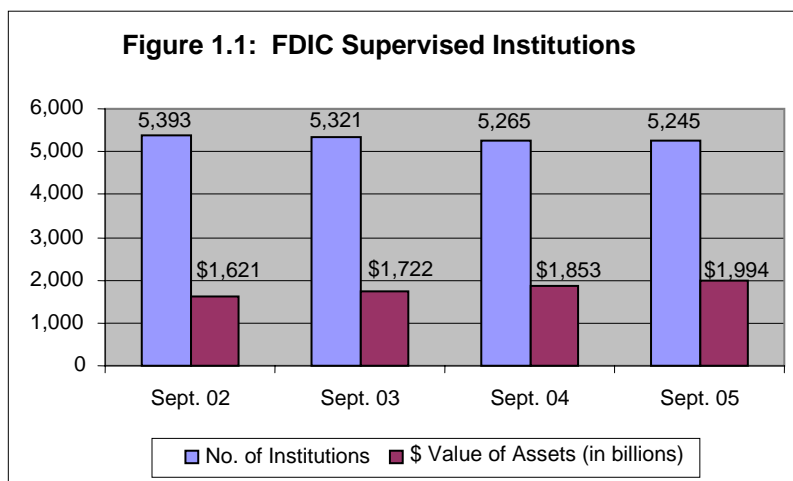
performs safety and soundness, Bank Secrecy Act (BSA), IT, trust, and other types of specialty examinations of FDIC-supervised insured depository institutions. The majority of the states participate with the FDIC in an examination program under which certain examinations are performed on an alternating basis by the state regulators and the FDIC. The examinations are conducted to assess an institution's overall financial condition, management practices and policies, and compliance with applicable laws and regulations.

The banking industry has taken on added complexity in the past decade, which can be attributed to the consolidation of the industry, the impact of globalization, and the development of increasingly complex investment strategies available to banks. This has led bank regulators,

both domestically and internationally, to devise new standards for bank capital requirements commonly referred to as Basel IA and Basel II. The FDIC has been engaged with other bank regulators in developing new standards and assessing the potential impact on bank safety and soundness.

In addition, the FDIC is faced with developing and implementing programs to minimize the extent to which the institutions it supervises are involved in or victims of financial crimes and other abuse. Bank governance practices are important safeguards against fraud and

other abuses, 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. In its role as supervisor, the FDIC also analyzes data



The Corporation also has back-up examination authority to protect the interests of the deposit insurance funds for more than 3,609 (as of September 30, 2005) national banks, state-chartered banks that are members of the Federal Reserve System, and savings associations. The FDIC also

security threats, occurrences of bank security breaches, and incidents of electronic crime that involve financial institutions. As part of BSA examinations, the FDIC also ensures that the institutions comply with regulatory reporting requirements.

The FDIC has to facilitate the effective implementation of regulatory reporting requirements without imposing any undue regulatory burden. As more and more laws are passed, and new regulations are adopted to implement those laws, it is incumbent upon policy makers and regulators to ensure that the intended benefits justify the considerable costs. The regulators need to take stock periodically of the cumulative effect of all regulatory requirements on the industry. As Federal Reserve Board Chairman Alan Greenspan said in a speech a few months ago, “to be effective regulators we must also attempt to balance the burdens imposed on banks with the regulations’ success in obtaining the intended benefits and to discover permissible and more efficient ways of doing so.” Pursuant to the Economic Growth and Regulatory 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.

The OIG’s role under this strategic goal is targeting audits and evaluations that review the effectiveness of various FDIC programs aimed at providing continued stability to the nation’s banks. The OIG also conducts investigations of fraud at FDIC-supervised institutions; fraud by bank officers, directors, or other insiders; obstruction of bank examinations; fraud leading to the failure of an institution; fraud impacting multiple institutions; and fraud involving monetary losses that could significantly impact the institution.

**2006 Performance Goals:** To assist the FDIC to ensure the nation’s banks operate safely and soundly, the OIG will

- Evaluate the effectiveness of the FDIC’s Supervision Program, and
- Evaluate and assist FDIC efforts to detect and prevent bank secrecy violations, fraud, and financial crimes in FDIC-insured institutions.

---

## ***2006 Performance Goal 1.1:*** ***Ensure the effectiveness of the FDIC’s supervision program.***

### **Key Efforts**

- Conduct material loss reviews and report on failures of FDIC-supervised 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.
- Determine whether the FDIC’s examinations comply with applicable policies and procedures for addressing an institution’s sensitivity to interest rate changes and also evaluate the FDIC activities that contribute to the assessment of interest rate risk.
- Determine whether the FDIC’s examination procedures address the risks associated with electronic banking and the extent to which examiners follow those procedures.
- Determine whether the FDIC’s examinations assess the reliability of appraisals as part of the evaluation of an institution’s lending policies and practices.
- Investigations involving obstruction of bank examinations.

## Significance

In accordance with section 38(k) of the Federal Deposit Insurance (FDI) Act, the cognizant OIG will 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. The general purpose of these reviews is to identify what caused the material loss, evaluate the supervision of the federal regulatory agency (including compliance with the “Prompt Corrective Action” requirements of the FDI Act), and propose recommendations to attempt to prevent a recurrence. 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. In 2005, for the first year in recent history, no banks or thrifts failed in the United States, and thus, no material loss reviews were performed.

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 intentional denial of accurate information to bank examiners undermines the integrity of this process. The OIG defends the vitality of the FDIC’s examination program by investigating allegations of criminal obstruction of bank examinations and by working with U.S. Attorneys’ Offices to bring these cases to justice.

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.

In 2006, the OIG is focusing on how effective the FDIC’s examinations are in assessing certain types of risks that can be particularly sensitive for banks. In one audit, we are focusing on an assessment of interest rate risks. Many of the financial institutions supervised by the FDIC have significant amounts of interest-sensitive securities in their investment portfolios. A bank’s participation in the sale or purchase of derivatives, interest rate swaps, and hedging activities involves sophisticated risks directly susceptible to rate changes that can result in rapid declines in value. This, in turn, can put the safety and soundness of the institution, and the deposit insurance funds, at risk.

Similarly, the OIG will review added risks associated with electronic banking, and how the FDIC has addressed those risks. Financial institutions are increasingly aggressive in adopting electronic banking capabilities, but these capabilities carry new and unique risks. FDIC examinations must consider many risk factors, including security, authentication processes, losses from fraud, customer privacy, and customer satisfaction. Our planned work will determine whether examination procedures adequately address the risks associated with electronic banking and the extent to which the examiners follow the procedures.

Banks often are involved with loans with real estate held as collateral. A bank’s risk depends primarily on the loan amount in relation to the collateral value, the interest rate, and most importantly, the borrower’s ability to repay. Banks rely on appraisals as one means to determine the value of collateral. The OIG plans an audit to determine whether the FDIC’s examinations adequately assess the reliability of appraisals.

## Potential Outcomes

- 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.
- Improved use of appraisals in evaluating the institution's lending practices.
- Detection of bank examination obstruction and prosecution of those responsible.

## 2006 Performance Goal 1.2:

*Assist FDIC efforts to detect and prevent bank secrecy violations, fraud, and financial crimes in FDIC-insured institutions.*

### Key Efforts

- Conduct investigations based on allegations of fraud at open FDIC-supervised institutions and closed institutions.
- Determine whether the FDIC is adequately using the Financial Crimes Enforcement Network (FinCEN) data and tools in assessing the BSA and anti-money laundering programs of FDIC-supervised institutions.
- Determine the extent to which FDIC examiners are following BSA examination procedures for foreign transactions.

### Significance

The reality today is that all financial institutions are at risk of being used to facilitate criminal activities, including money laundering and terrorist financing. A challenge for the Corporation is ensuring that the institutions it supervises are not involved in or victims of financial crimes and other abuse. 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. Fraud has been a contributing factor in virtually all bank failures in recent years.

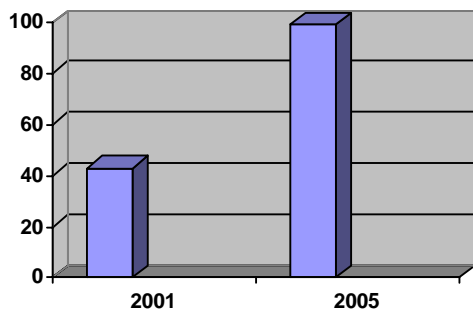
The OIG's Office of Investigations works closely with FDIC management in the Division of Supervision and Consumer Protection (DSC) to identify and investigate financial institution crime,

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. Another consideration in dedicating OIG resources to these cases is the need to pursue appropriate criminal penalties not only to punish the offender but to deter others from participating in similar crimes.

Since the terrorist attacks of September 11, 2001, the FBI, which historically had taken the lead in investigating financial institution fraud, has no longer been able to devote the same level of resources to these cases. The OIG fully expects its caseload of financial institution fraud to continue to increase. Based on our past success, U.S. Attorneys' Offices and FBI Offices throughout the country are increasingly relying on the FDIC OIG as a significant resource. Referrals and requests for investigative assistance from the U.S. Attorneys'

Offices and the FBI are on the increase, and the OIG expects that trend to continue. The OIG is also receiving more referrals of financial institution fraud matters from DSC. Given the level of collaboration currently ongoing with DSC, the OIG expects these 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 OIG's investigations of financial institution fraud currently constitutes 72 percent of the OIG's investigation caseload. As shown in Figure 1.2, at year end 2001, the OIG had 43 open financial institution fraud cases. That number had risen to 99 by year-end 2005.

**Figure 1.2: OIG Financial Institution Fraud Caseload**



Source: OIG Data

Since the passage of the USA PATRIOT Act (Uniting and Strengthening America by Providing

**Potential Outcomes**

- Reduced opportunity for fraud to take place within financial institutions.
- The FDIC recovers its losses from financial institution fraud and avoids further harm.
- Criminal penalties are assessed where appropriate, and others are deterred from participating in similar crimes.
- Improved detection and remedies to identify BSA violations and money laundering activities.

Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001), the FDIC has been actively engaged in a number of BSA, anti-money laundering, and counter-financing of terrorism initiatives. During the past year, the FDIC contributed to joint industry and interagency working groups for the development of rules and interpretive guidance, and incorporated rules and guidance into examination procedures and industry resources.

Although the Treasury Department has overall authority for BSA enforcement and compliance, FinCEN, created in 1990, has delegated authority to administer the BSA. 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 Suspicious Activity Reports (SARs) when suspected money laundering or BSA violations occur. FinCEN maintains at least two automated systems from which DSC examiners should download information on CTRs and SARs filed by FDIC-supervised institutions—the Currency and Banking Retrieval System and the Currency and Banking Query System. The filing and use of SARs and CTRs has been the subject of significant regulatory, congressional, and banking community interest.





## **Strategic Goal 2: Help the FDIC Maintain the Viability of the Insurance Funds**

FDIC deposit insurance remains a central component of the federal government's assurance to the public that it can be confident in the stability of the Nation's banks and savings associations. Since its establishment in 1933, the FDIC has insured deposits up to the legally authorized threshold, which presently stands at \$100,000. For almost two decades following bank crises in the late-1980's and early 1990's, the FDIC has managed two deposit insurance funds—one for banks with about \$35 billion, and one for savings and loans with about \$13 billion. These funds, which are primarily an accumulation of premiums that insured depository institutions have paid the FDIC and interest earned, have been used to pay FDIC operating expenses and insured depositors, as necessary.

Legislation passed by the Congress on February 1, 2006, changes how the FDIC manages deposit insurance. The legislation:

- Merges the BIF and SAIF into a single Deposit Insurance Fund.
- Maintains deposit insurance coverage for individual accounts at \$100,000, but provides for indexing for inflation every 5 years beginning in 2010.
- Increases deposit insurance coverage for retirement accounts to \$250,000 and provides for indexing for inflation every 5 years beginning in 2010.
- Replaces the current Designated Reserve Ratio of 1.25 percent of estimated insured deposits by permitting the reserve ratio to move within a range of 1.15 percent to 1.50 percent of estimated insured deposits.

- Requires the FDIC to provide cash rebates in amount equaling 50 percent of the amount in excess of the amount required to maintain the reserve ratio at 1.35 percent. Requires the FDIC to provide cash rebates in amount equaling the total amount in excess of the amount required to maintain the reserve ratio at 1.50 percent.
- Provides financial institutions with a one-time transitional premium assessment credit based on the assessment base of the institution on December 31, 1996, as compared to the combined aggregate assessment base of all eligible depository institutions.

The Corporation is now working to implement the provisions of the new legislation.

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 funds. Financial instruments and transactions continue to become more complex, and the process of financial intermediation, even in smaller institutions, increasingly sophisticated. Further, the ongoing consolidation of the banking industry means that there are a few very large institutions that represent an increasingly significant share of the FDIC's exposure. According to the Corporation, as of September 30, 2005, the ten largest FDIC-insured institutions accounted for 42 percent of deposits and 43 percent of the assets of all FDIC-insured institutions. 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.

**2006 Performance Goals:** To help the FDIC maintain the viability of the insurance funds, the OIG will

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

- Assess the management of the deposit insurance funds.

---

## **2006 Performance Goal 2.1:**

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

### **Key Efforts**

- Audit coverage of the FDIC's approach to assessing and addressing risks posed to the insurance funds by large or multiple bank failures.
- Evaluate the FDIC's risk-based premium assessment process.
- Evaluate the FDIC's process for reviewing and investigating industrial loan company applications for deposit insurance and determine whether the process fully considers statutory and applicable factors.

### **Significance**

The continuing consolidation of the financial services industry has resulted in fewer and fewer financial institutions controlling an ever-expanding percentage of the nation's financial assets. 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. As insurer, the FDIC needs insight into the risks that are inherent in U.S. banking organizations. As of June 30, 2005, the 25 largest banks controlled \$5.64 trillion, or 54 percent, of total bank assets in the country. The FDIC is the primary federal regulator for only 3 of these 25 financial institutions. The OIG has previously reported on the importance of the FDIC's back-up examination authority to carry out its responsibilities. In recent years, the FDIC has taken a number of measures to strengthen its oversight of the risks to the insurance funds posed by the largest and most complex institutions, and its key programs include:

- Large Insured Depository Institution Program,

- Dedicated Examiner Program,
- Shared National Credit Program, and
- Off-site monitoring systems.

The OIG plans to develop a strategy for its audit coverage of the FDIC's approach to assessing and addressing risks posed to the insurance funds by large and multiple bank failures, the latter reflecting the reality of a regional disaster and its significant impact on a large number of financial institutions. We envision a series of audits that will address the key programs and activities in this area.

The FDIC has a system to charge higher premiums on a limited basis, or in recent years, to charge premiums only to financial institutions that pose greater risk. Deposit insurance reform will provide the FDIC with even more authority to assess risk-based premiums. This authority enables the FDIC to charge insurance premiums tied more to risks much like private insurance companies charge premiums. In order to assess these premiums, the FDIC needs a system to fairly ascertain the risks posed by an institution and to levy a fair premium.

Our audit work in this area is reviewing whether the FDIC system for charging premiums is adequately tied to risks identified in recent bank examinations. This effort may have significant implications as the FDIC goes forward to implement new authorities.

The FDIC is the only federal agency with the authority to approve institutions' applications for deposit insurance under the Federal Deposit Insurance Act. The FDIC must evaluate factors specified by Section 6 of the Federal Deposit

Insurance Corporation Improvement Act to determine what type of risk the new institution would pose to deposit insurance funds. Apart from safety and soundness and compliance factors, the FDIC must evaluate the applications of business organizations who are seeking deposit insurance for de novo financial institutions. These proposals involving industrial loan companies and credit card banks often require the imposition of additional conditions prior to approval in order to preserve the integrity of the insurance funds.

### Potential Outcomes

- Improved risk management at large U.S. banks.
- Insurance premiums commensurate with the level of risk posed to the deposit insurance funds by a bank's business practices and conditions.
- Insurance application decisions that fully consider risks.

---

## **2006 Performance Goal 2.2:** *Assess the management of the deposit insurance funds.*

### Key Effort

- Review the assessment process and calculation of the deposit insurance funds' ratio to insured deposits

### Significance

Deposit insurance fund premium assessments have historically been prescribed by the Federal Deposit Insurance Corporation Improvement Act of 1991. The act directs the FDIC to implement a limited risk-based insurance system and to maintain insurance fund reserves of 1.25 percent to estimated insured deposits. (The deposit insurance reform legislation provides the FDIC more discretion on the reserve ratio and impacts the risk assessment

process.) To implement the fund ratio at the appropriate level, the FDIC has depended on its Division of Finance to accurately calculate, collect, and process assessments and to properly determine the reserve ratio in the insurance funds to insured deposits. When the reserve ratio falls below the designated level, a premium assessment may be required.

### Potential Outcomes

- Better information on which to base assessment decisions.
- More successful implementation of deposit insurance reforms.



## **Strategic Goal 3:**

### **Assist the FDIC to Protect Consumer Rights and Ensure Community Reinvestment**

The U.S. Congress has long advocated particular protections for consumers in relationships with banks. Federal fair lending and consumer protection laws, such as the Fair Housing Act, the Equal Credit Opportunity Act, Gramm-Leach-Bliley Act, the Fair and Accurate Credit Transaction Act, the Truth in Lending Act as amended by the Home Ownership and Equity Protection Act, and the Real Estate Settlement Procedures Act provide substantive protection to borrowers. These laws provide disclosure requirements, define high-cost loans, and contain anti-discrimination provisions. To help monitor the home lending market, the Federal Reserve and other bank regulators, such as the FDIC, collect and monitor loan pricing data in accordance with the Home Mortgage Disclosure Act (HMDA). The purpose behind getting the data is to enable bank regulators, including the FDIC to conduct efficient fair lending reviews and to make sure banks are providing equal access and pricing for loans regardless of a borrower's racial or ethnic background. The Congress has also enacted the Community Reinvestment Act (CRA) of 1977 to encourage federally insured banks and thrifts to help meet the credit needs of their entire community, including low- and moderate-income neighborhoods, consistent with safe and sound operations. The CRA requires federal bank regulators to assess each insured institution's record of meeting these needs.

The FDIC oversees statutory and regulatory requirements aimed at protecting consumers from unfair and unscrupulous banking practices. The FDIC has recognized the importance of its role in this regard by establishing its own strategic goal to

ensure 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 their compliance with laws and regulations governing consumer protection, fair lending, and community investment. A principal effort at consumer education has been the FDIC's *Money Smart* program that aims to provide basic financial education skills to current and potential bank customers, often through alliances with government, charitable, and community development organizations.

The FDIC's bank examiners conduct examinations in FDIC-supervised banks on a scheduled basis to determine the institutions' compliance with laws and regulations governing consumer protection, fair lending, and community investment. When problem institutions are identified, primarily through the examination process, the FDIC attempts using reason and moral suasion to bring about corrective actions; however, the Corporation possesses broad enforcement powers to correct situations that threaten an institution's compliance with applicable laws.

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.

**2006 Performance Goals:** To assist the FDIC to protect consumer rights and ensure community reinvestment, the OIG will

- Evaluate the effectiveness of FDIC programs for protecting consumer privacy,

- Review FDIC’s fair lending and community reinvestment examination programs, and
- Strengthen enforcement against misrepresentations of deposit insurance coverage.

## **2006 Performance Goal 3.1:** *Evaluate the effectiveness of FDIC programs for protecting consumer privacy.*

### **Key Efforts**

- Assess the FDIC's examination coverage of bank service providers' protection of sensitive customer information.
- Determine whether DSC has provided adequate institution and examination guidance for implementing the data privacy and security provisions of Title V of the Gramm-Leach-Bliley Act and the Fair and Accurate Credit Transaction Act, and implemented prior OIG recommendations.
- Determine whether the Division of Resolutions and Receiverships (DRR) adequately protects personal information collected and maintained for resolution and receivership functions.
- Determine the extent to which the FDIC IT examinations ensure that FDIC-supervised institutions are adequately protecting consumer data.
- Determine whether FDIC examinations are effectively assessing the data security risks associated with offshore outsourcing.
- Conduct investigations involving “Phishing,” “Pharming,” and other identity theft schemes.
- Review and comment on proposed FDIC policies and procedures for protecting financial data privacy.

### **Significance**

Data security and financial privacy are important values in American society. The Congress has recently enacted several laws designed to further these values in banks and other financial institutions. Despite congressional efforts, regulations promulgated by federal agencies such as the FDIC, and added emphasis by law enforcement, identity theft is becoming more sophisticated and the number of victims is growing.

<b>Table 3.1: Costs of ID Theft in 2005</b>	
Percent of Population Victimized	4.25%
Number of Victims	9.3 million
Annual Cost	\$52.6 billion
Hours Victims Spent Resolving	260.4 million

Source: Javelin Strategy & Research, 2005 Identity Fraud Survey Report

In fact, the FDIC has been recognized as a leader in publicizing the risks of identity theft to both banks and the public. The FDIC's publication, *Putting an End to Account-Hijacking and Identity Theft*, led to an FDIC-sponsored symposium bringing together expert representatives from federal and state government, the banking industry, consumer interest groups, and law enforcement. Innocent victims of identity theft sometimes suffer serious losses. If the crime is not detected early, people face months or years cleaning up the damage to their reputation and credit rating, and sometimes they lose out on loans, jobs, and other opportunities in the meantime.

Identity theft includes using the Internet for new crimes such as "phishing" e-mails and "pharming" Web sites that attempt to trick people into divulging their private financial information by pretending to be legitimate businesses or government entities with a need for the information that is requested. OIG audits and evaluations will be designed to focus on the issues and determine the effectiveness of the FDIC's strategies and its implementation of programs and activities to protect consumer privacy. OIG criminal investigations will give priority to exposing those who illegally seek and use stolen identifications from FDIC-supervised banks and their affiliates and bringing them to justice.

### Potential Outcomes

- Enhanced security of customer information maintained by financial institutions and their servicing agents.
- Improved agency implementation of the data privacy and security provisions of the Gramm-Leach-Bliley Act and the Fair and Accurate Credit Transaction Act.
- Enhanced protection of personal information collected and maintained by DRR for resolution and receivership functions.
- Reduced opportunity for illegal "phishing," "pharming," and other identify theft schemes that threaten our financial institutions and their customers, and justice for the perpetrators.

---

## ■ **2006 Performance Goal 3.2:** *Review the FDIC's fair lending and community reinvestment examination programs.*

### Key Efforts

- Evaluate the FDIC's approach to fair lending examinations when a financial institution uses credit scoring systems.
- Determine the challenges faced and the effectiveness of efforts taken by the FDIC to identify, assess, and address the risks posed to institutions and consumers from predatory lending practices.
- Assess how the FDIC makes use of available HMDA data to identify and assess instances of potential discrimination when examining an institution's compliance with relevant laws and regulations.
- Determine the effect that the new interagency CRA regulations have had on the FDIC's ability to assess each federally insured institution's record of helping to meet the credit needs of its entire community, consistent with safe and sound lending, and assess how the FDIC is measuring and reporting on the effectiveness of the new procedures.

- Determine whether the FDIC adequately addresses the violations and deficiencies reported in compliance examinations to

ensure that FDIC-supervised institutions take appropriate corrective action.

### Significance

Over the past 20 years, the nation has made significant progress in expanding access to capital for previously under-served borrowers. Subprime lending provides loans to borrowers who do not meet credit standards for what the credit industry considers prime lending. However, some borrowers in the subprime market may be particularly vulnerable to abusive lending practices known as “predatory lending.” These practices involve engaging in deception or fraud, or taking unfair advantage of a borrower’s lack of understanding about loan terms. Unfortunately, predatory lending often occurs in the subprime mortgage market where borrowers use the collateral in their homes for debt consolidation or other consumer credit purposes.

In other forms, lenders may provide high-cost, short-term credit on a recurring basis to customers with long-term credit needs. In September 2005, the FDIC held a roundtable with those banks it supervises with outstanding CRA records to identify responsible alternatives for meeting short-term consumer credit needs.

The line between legitimate and predatory subprime loans is often fuzzy. To help monitor the home lending market, the Federal Reserve collects and monitors loan pricing data in accordance with HMDA. The purpose behind getting the data is to enable bank regulators, including the FDIC, to conduct efficient fair lending reviews and to make sure banks are providing equal access and pricing for loans regardless of a borrower’s racial or ethnic background. Recent data shows higher denial rates and prices for minorities than non-minorities, but the Federal Reserve reports that adjusting the data

for factors such as loan amount, borrower income, and the type of institution doing the lending narrows the gap. However, the Federal Reserve also reports that it is clear some lenders were taking advantage of their customers. Federal fair lending and consumer protection laws, such as the Fair Housing Act, the Equal Credit Opportunity Act, the Truth in Lending Act as amended by the Home Ownership and Equity Protection Act, and the Real Estate Settlement Procedures Act also provide substantive protection to borrowers. These laws provide disclosure requirements, define high-cost loans, and contain anti-discrimination provisions.

The Congress has also enacted CRA to encourage federally insured banks and thrifts to help meet the credit needs of their entire community, including low- and moderate-income neighborhoods, consistent with safe and sound operations. The CRA requires federal bank regulators to assess each insured institution’s record of meeting these needs. Recently revised regulations relieved smaller institutions from some requirements.

The FDIC carries out its responsibilities associated with fair lending and CRA compliance examinations at banks where it is the primary federal regulator on a scheduled basis. Because maintaining a balance between consumers’ credit access, community investment, and prevention of abusive lending practices is important to millions of Americans and is a priority for the FDIC, the OIG has established a performance goal for reviewing the FDIC’s programs for fair lending and community reinvestment examinations.

### Potential Outcomes

- More effective fair lending examinations and greater assurance that financial institutions comply with the Equal Credit Opportunity Act when using credit scoring systems to evaluate a borrower’s creditworthiness.
- Improved protection for consumers from predatory and other unfair lending practices.
- Improved protection for homeowners and homebuyers from predatory lending practices, including price discrimination,

when applying for housing loans covered by HMDA.

- Improved effectiveness of the Corporation's CRA examination program.

- A more effective enforcement program to ensure that FDIC-supervised institutions comply with fair lending, privacy, and various other consumer protection laws and regulations.

---

## **2006 Performance Goal 3.3:** *Strengthen enforcement against misrepresentations of deposit insurance coverage.*

### **Key Efforts**

- Conduct investigations of alleged schemes that mislead consumers about rates of return on deposits through misuse of FDIC's name, logo, abbreviation, or other indicators that wrongly suggest deposits are insured.
- Work with FDIC management and the Congress to enhance the FDIC's enforcement authority for misrepresentations regarding FDIC insurance.

### **Significance**

OIG investigations have recently identified multiple schemes to defraud depositors by offering them misleading rates of return on deposits. These abuses are effected through the misuse of the FDIC's name, logo, abbreviation, or other indicators suggesting the products are fully insured deposits. Such misrepresentations induce the targets of schemes 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. OIG semiannual reports to the Congress provide information on cases that have

been successfully investigated involving these types of misrepresentations, including one case of \$9.1 million worth of certificates of deposit misrepresented to about 90 investors, most of whom were elderly.

The FDIC currently has no direct enforcement authority over these misrepresentations. The FDIC may, of course, generally address misconduct occurring in state chartered banks where the FDIC is the primary federal regulator, but the abuses described above generally were perpetrated outside of that system. The OIG has proposed strengthening the FDIC's enforcement authority to curtail these abuses by granting the FDIC the authority to impose civil monetary penalties of up to \$1 million per day on any person who falsely represents the nature of the product offered or the FDIC insurance coverage available.

### **Potential Outcomes**

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





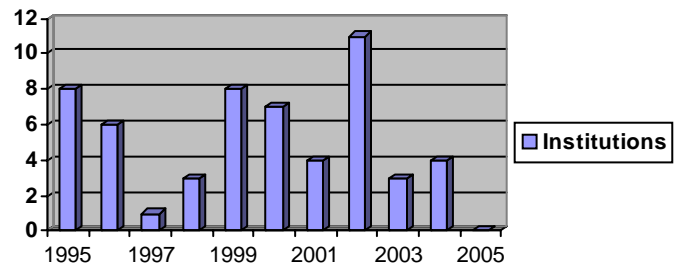
## Strategic Goal 4: Help Ensure that the FDIC is Ready to Resolve Failed Banks and Effectively Manages Receiverships

When a bank that offers federal deposit insurance fails, the FDIC fulfills its role as insurer by either facilitating the transfer of the institution's insured deposits to an assuming institution or by paying insured depositors directly. Specifically, the FDIC's DRR mission is 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 the financial system.

Once an institution is closed by its chartering authority—the state for state-chartered institutions, the Office of the Comptroller of the Currency for national banks, and the Office of Thrift Supervision for federal savings associations—the FDIC is responsible for resolving the failed bank or savings association. The FDIC begins the resolution process with an assessment of the assets and liabilities of the institution. Using this information, DRR solicits proposals from approved bidders to pass the insured deposits to an assuming bank and expedite the return of assets to the private sector. Once the FDIC is appointed receiver, it initiates the closing process for the failed institution and works to provide the insured depositors with access to their accounts in 1 or 2 business days. To accomplish this, the FDIC works with the assuming institution so that the insured deposit accounts are transferred to the assuming institution as soon as possible.

If no assuming institution is found during the resolution process, the FDIC disburses to customers of the failed institution the insured amount in each

**Figure 4.1: Number of Closings and Assistance Transactions**



Source: FDIC Historical Statistics on Banking

account category. The FDIC, as receiver, manages the receivership estate and the subsidiaries of failed financial institutions with the goal of achieving an expeditious and orderly termination.

Since the FDIC's inception over 70 years ago, no depositor has ever experienced a loss of insured deposits at an FDIC-insured institution due to a failure. Today record profitability and capital in the banking industry have led to a substantial decrease in the number of financial institution failures and near failures than were experienced in prior years. In fact, 2005 was the first year in the FDIC's history where no institution has failed. Although there have been far fewer failures in recent years than occurred during the years of crisis in the banking industry, the FDIC's responsibility for resolving troubled institutions remains a challenge. The FDIC reports that failures in today's economy would differ in nature, size, and cost from the record failures of the 80s and early 90s. Nonetheless, 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 or have to handle multiple failures caused by a single catastrophic event like Hurricane Katrina.

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.

**2006 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 failures, and
- Assist the FDIC in recovering financial losses from individuals fraudulently concealing assets.

**2006 Performance Goal 4.1:**  
*Evaluate the FDIC’s plans and systems for managing bank failures.*

**Key Efforts**

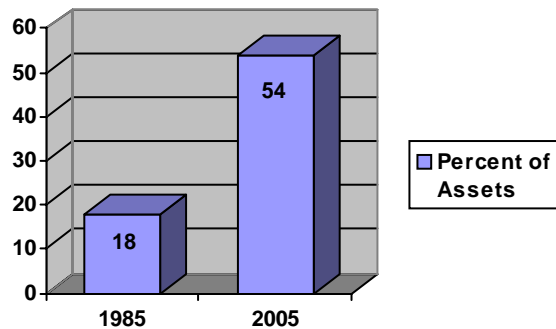
- Assess the effectiveness of the FDIC’s planning for large or multiple bank failures.
- Review the development framework for the Asset Servicing Technology Enhancement Project (ASTEP).
- Determine whether FDIC systems accurately track and obtain recovery of unclaimed deposits after institution failures.

**Significance**

The consolidation of banks serving different product and geographic markets helps to diversify risk and decrease earnings volatility, thereby decreasing the likelihood of failure. Historically, very few failures have occurred among the nation’s largest banks. Since 1934, only 2 failures occurred among the nation’s top 25 banking organizations. Only six bank failures ever involved institutions with more than \$10 billion in assets.

Nonetheless, since the mid-1980s, consolidation within the industry has reduced the number of federally-insured banks and thrifts from over 18,000 to less than 8,900. The FDIC forecasts that industry consolidation will continue to decrease the aggregate number of insured depository institutions, and concentration of risk to the insurance funds in the largest bank organizations will grow more pronounced over time.

**Figure 4.2: Share of Industry Assets Held by 25 Largest Insured Institutions**



Source: FDIC

The potential impact to the deposit insurance funds from the failure of a single, large consolidated institution is greater. Moreover, although no

institution has failed because of a natural disaster, the FDIC must be prepared to respond to potential problems that can arise from wide-spread natural disasters or other unprecedented events that could impact the viability of multiple financial institutions.

The FDIC is taking steps to address the challenges posed by these particular scenarios. Specifically, DRR has and continues to develop and/or update plans to handle a number of different contingencies, including the possible failure of large institutions, Internet banks, and/or simultaneous multiple failures. Contingency plans center on resolution methods and staffing alternatives. For example, the FDIC is in the midst of a multi-year effort to redesign and automate its deposit insurance claims and payment process. This process redesign effort is aimed at providing an integrated solution that meets the Corporation's current and future deposit insurance determination needs. Additionally, in 2004, the FDIC established the Resolutions Policy Committee and supporting subcommittees to ensure the FDIC achieves a maximum state of readiness to deal with the potential or actual failure of the nation's largest insured depository institutions. The Resolution Policy Committee has recently completed a plan for handling a large bank failure. Furthermore, the Corporation implemented the Corporate Employee Program. This program is designed to expand the FDIC's knowledge base in the areas of resolutions and receiverships and will ensure a continual level of readiness among the workforce by promoting cross-divisional mobility through continuous training and rotational work assignments.

### Potential Outcomes

- Continued distribution of insured deposits in a timely and accurate manner to customers of failed banks.
- Maximum recovery of assets and unclaimed deposits for the FDIC and other creditors of failed financial institutions.
- Improved state of readiness for dealing with various potential scenarios related to large or multiple financial institution failures, including increased coordination with other federal banking regulatory agencies, enhanced risk management, and effective staffing solutions.

Additionally, a key component in the FDIC's plan for managing future bank failures is the development of new technology for managing receivership functions. The project called ASTEP focuses on outsourcing work and using integrated computer software to support the FDIC's asset serving role when banks are placed into receivership status.

The 1993 Unclaimed Deposits Amendment Act gives account owners 18 months to claim their deposits after the failure of a financial institution. At the end of the 18-month period, the FDIC transfers unclaimed deposits for failed FDIC-insured financial institutions to the appropriate state unclaimed property agency of the owner's last known address.

The state maintains custody of the funds in accordance with its unclaimed property laws for 10 years from the date the FDIC transferred the funds. After the 10-year holding period, state unclaimed property agencies must return any unclaimed funds to the FDIC. DRR estimates that by 2015, unclaimed funds due to the FDIC will total more than \$25 million. The FDIC needs to ensure that adequate systems are in place to accurately track and obtain the recovery of these unclaimed deposits.

In 2006 the OIG will focus attention on evaluating the effectiveness of the FDIC's program and activities aimed at ensuring it can handle large bank failure or multiple bank failures, its development of ASTEP, and its efforts to recover unclaimed deposits.

## **2006 Performance Goal 4.2:**

*Assist the FDIC in recovering financial losses from individuals fraudulently concealing assets.*

### **Key Efforts**

- Continue regular meetings with DRR and Department of Justice officials to identify potential instances of fraudulently concealed assets.
- Conduct criminal investigations, identify concealed assets for seizure, and pursue judicial remedies, if appropriate.

### **Significance**

The FDIC was owed more than \$1.7 billion in criminal restitution as of September 30, 2005. 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. The OIG's Office of

Investigations works closely with DRR and the Legal Division in aggressively pursuing criminal investigations of these individuals. At January 1, 2006, the OIG had 19 open cases regarding potential restitution fraud against the FDIC.

### **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: Promote Sound Governance and Effective Stewardship of Financial, Human, IT, and Procurement Resources

The FDIC must effectively manage and utilize a number of critical strategic resources in order to carry out its mission successfully, particularly its financial, human, IT, and procurement 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. In articulating the corporate priorities for 2003, former FDIC Chairman Donald Powell identified Stewardship —“Stewardship of the Corporation and insurance funds to ensure that the FDIC does its job in the most efficient and effective manner possible.” It has remained a corporate priority since that time. And, in fact, one of the FDIC’s own core values articulates its commitment to financial stewardship, as follows: *The FDIC acts as a responsible fiduciary, consistently operating in an efficient and cost-effective manner on behalf of insured financial institutions and other stakeholders.*

A brief discussion of the budgeting practices of the FDIC helps put its financial operations, **fiduciary responsibilities**, and related decision-making in context.

The FDIC Board of Directors approves an annual Corporate Operating Budget to fund the operations of the Corporation. The Corporate Operating Budget consists of two components, Ongoing Operations and Receivership Funding. The

Receivership Funding component of the operating budget includes funds for all resolutions and receivership management activities, except the costs associated with maintaining the core staff that performs these functions regardless of the level of failure activity.

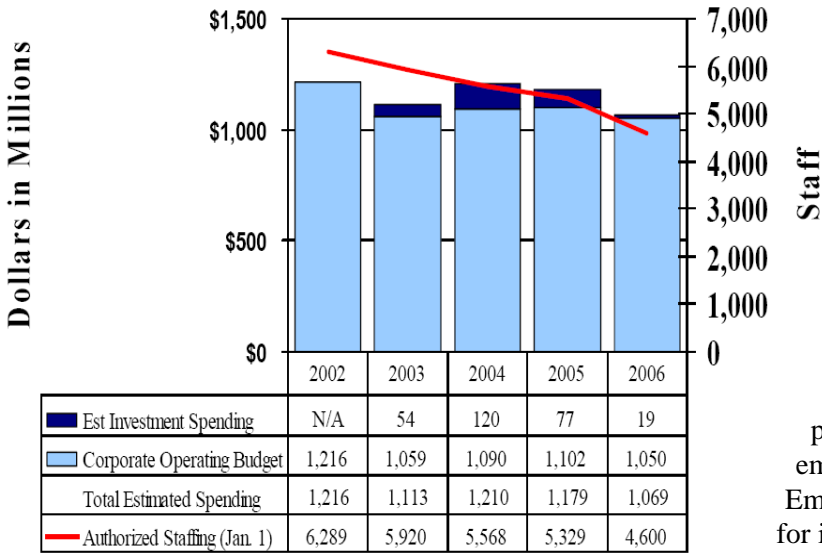
The FDIC’s separate Investment Budget is composed of individual project budgets approved by the Board of Directors for major investment projects. Budgets for investment projects are approved on a multi-year basis, and funds for an approved project may be carried over from year to year until the project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

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.

Expenditures from the Corporate Operating and Investment Budgets have been paid from three funds managed by the FDIC—the Bank Insurance Fund (BIF), the Savings Association Insurance Fund (SAIF), and the FSLIC Resolution Fund (FRF). The BIF and the SAIF are funded by deposit insurance premiums paid by insured financial institutions as well as interest earned on the investment of those funds, while the FRF consists of public funds appropriated by the Congress. In

addition, receiverships managed by the Corporation reimburse the insurance funds for services provided by the FDIC. The Corporation’s 2006 spending is expected to total approximately \$1.069 billion. Figure 5.1 contains a 5-year overview of FDIC’s total spending.

**Figure 5.1: Five-Year Overview of FDIC Spending 2002 - 2006**



Source: FDIC’s Summary Statistics Report-November 2005

Financial resources are but one aspect of the FDIC’s critical assets. The Corporation’s **human capital** is also vital to its success. The Government Accountability Office has reported that to attain the highest level of performance and accountability, an agency’s people are its most important aspect because they define the agency’s character and ability to perform. GAO has issued a number of products encouraging agencies to focus on valuing employees and aligning their people policies to support organizational performance goals. GAO identified four key human capital cornerstones for effective management of human capital: Leadership; Strategic Human Capital Planning; Acquiring, Developing, and Retaining Talent; and Performance Culture.

GAO has not been the only voice promoting human capital management. In August 2001, the President placed human capital at the top of his management agenda. The Office of Management and Budget (OMB), and the Office of Personnel Management

have subsequently been active in providing guidance and standards of success that emphasize the value of human capital policies and programs.

Turning attention again to the Corporation’s own core values, we see that the FDIC appreciates the importance of its people, with four of the six values, integrity, competence, teamwork, and fairness specifically referencing the workforce.

Technological advances have produced tools that all workers today would be lost without. **Information technology** 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.

Emerging technology is introducing new ways for insured depository institutions to deliver and manage traditional products and services, and, in some instances, to develop innovative offerings. Financial data is being exchanged at rapid speed and the business of banking is being greatly facilitated by modernization.

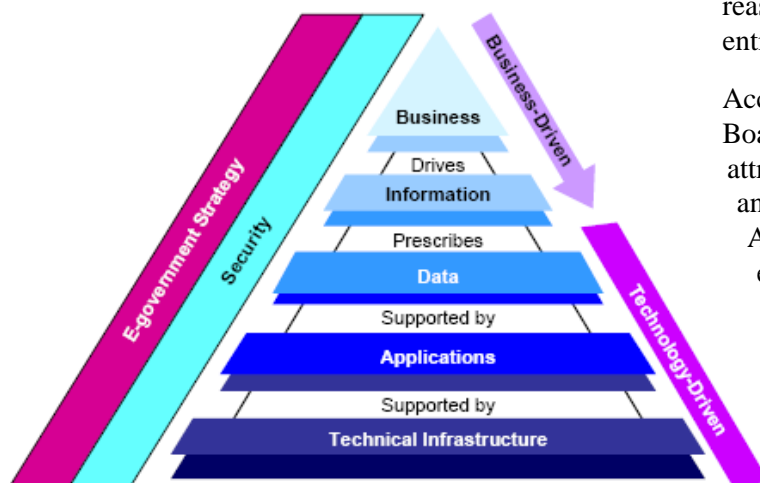
Along with the positive benefits that IT offers comes a certain degree of risk. In that regard, **information security** has been a long-standing and widely acknowledged concern among federal agencies. Since 1997, significant internal control weaknesses related to IT security, including untested contingency plans and inadequate implementation of host-network security, system risk assessments, system certification, and vulnerability testing have been identified. While agencies report a number of improvements in these areas, certain problems persist and more needs to be done.

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 II 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.

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 5.2.

**Figure 5.2: FDIC Enterprise Architecture**



Source: FDIC/Gartner, Inc.

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. The Corporation’s Acquisition Policy Manual contains guidance and uniform standards for

contracting for goods and services at the best value for the FDIC and was revised in May 2004.

According to the FDIC’s Purchase Order System, active purchase orders (that is, those contracts that have not been purged from the system due to inactivity for more than 2 years) from January 1, 1996 through March 22, 2004 totaled 7,243 contracts with a total purchase order base amount of \$2,640,000,000.

**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.”

According to a recent report by The Conference Board, the benefits that respondents to a survey attribute to ERM include better informed decisions and increased management accountability.

According to the report, companies that fully embrace ERM are better able to improve management practices such as strategic planning, and can better understand and weigh risk-reward equations in their decisions. The FDIC’s adoption of an ERM approach has great potential, if implemented appropriately.

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

- identify opportunities for more economical, efficient, and effective corporate expenditures of funds;
- recommend actions for more effective governance and risk management practices;
- 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; and
- ensure that procurement practices are fair, efficient, effective, and economical.

**2006 Performance Goals:** To promote sound governance and effective stewardship of FDIC strategic resources, the OIG will

- Evaluate the Corporation's efforts to fund operations efficiently, effectively, and economically.
- Assess the Corporation's human capital strategic initiatives to ensure a high-

performing work-force that views the FDIC as an employer of choice and that stands ready to meet challenges in the banking industry.

- Promote maximization of IT resources for efficiency and effectiveness and ensure IT and physical security to protect all FDIC resources from harm.
- Evaluate the Corporation's contracting efforts to ensure goods and services are fairly, efficiently, and economically procured.
- Monitor corporate efforts to identify and analyze the FDIC risk environment and validate that a sound internal control environment is in place and working well.

---

## **2006 Performance Goal 5.1:**

*Evaluate the Corporation's efforts to fund operations efficiently, effectively, and economically.*

### **Key Efforts**

- Determine the extent to which salary costs are being appropriately classified in the corporate accounting system (the New Financial Environment), and result in management information that is current, complete, accurate, and consistent to support decision-making.
- Assess the integration of the FDIC's system development and IT capital investment processes to ensure the timely delivery of cost-effective systems that meet business needs.
- Evaluate the FDIC's use of the Government Performance and Results Act to manage performance, report performance results, and gauge program success.

### **Significance**

The FDIC's operating expenses are largely paid from the insurance funds, and consistent with good corporate governance principles, the Corporation must continuously seek to improve its operational efficiency. Because 65 percent of the FDIC's budget costs are personnel-related, a challenge to the Corporation is to ensure that budgeted resources are properly aligned with workload. With respect to capital investments, effective planning and management of IT and non-IT capital investments are mandated by Congress and by OMB for most

federal agencies. Although many of these laws and executive orders are not legally binding on the FDIC, the Corporation recognizes that they constitute best practices and has adopted them in whole, or in part. The underlying challenge is to carry out approved investment projects on time and within budget, while realizing anticipated benefits.

Realizing that the FDIC had outgrown its prior financial system, the Corporation took steps to create a new financial environment by procuring an



enterprise financial software, PeopleSoft Financials. The Corporation needed more real-time, cost-oriented reporting to enhance organizational efficiency. The new system is being implemented to centralize business rules and security requirements, reduce staff time spent on data reconciliations, enhance e-business and budgeting capabilities, improve institutional analysis, achieve more paperless processing, and enhance cost management information. The new financial environment will be critical to assist corporate decision makers in determining how much focus and money to budget for corporate programs and activities. The system needs to provide reliable and accurate cost data to support decisions.

Focusing on accountable, results-oriented management can help the FDIC operate effectively within a broad network that includes other federal bank regulators, state regulators, the Congress, trade groups, consumers, and the banking industry. Part of this focus is to create a culture that moves from outputs to results, stovepipes to matrixes, and an inward to an external focus. The Congress has sought to instill a greater focus on results throughout government with the Government Performance and Results Act of 1993. The President's Management Agenda also emphasizes results-oriented practices. The FDIC prepares strategic and performance plans, has Chairman's "initiatives," and reports annually on performance and accountability.

### Potential Outcomes

- Enhanced cost management practices.
- Strengthened controls over capital investment projects.
- Improved, results-oriented management across the FDIC.

## **2006 Performance Goal 5.2:** *Assess the Corporation's human capital strategic initiatives to ensure a high-performing work-force that views the FDIC as an employer of choice and that stands ready to meet challenges in the banking industry.*

### Key Efforts

- Evaluate the FDIC's conversion to a new discrimination complaint resolution tracking system.
- Determine the extent to which the FDIC's succession planning efforts identify and address future critical staffing and leadership needs.
- Evaluate the FDIC's policies, procedures, and practices for safeguarding personal employee information in hardcopy and electronic form.
- 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.

### Significance

In the last several years, the FDIC has undergone significant restructuring and downsizing in response to changes in the industry, technological advances, and business process improvements and, as with many government agencies, the FDIC anticipates a high-level of retirement in the next 5 years. The

steady decline in FDIC staffing from 1995 through 2004 is shown in Figure 5.3. Amidst such change, the Corporation must seek to maintain employee morale and positive employee-management relationships. To that end, the FDIC formulated a human capital strategy to guide the FDIC through

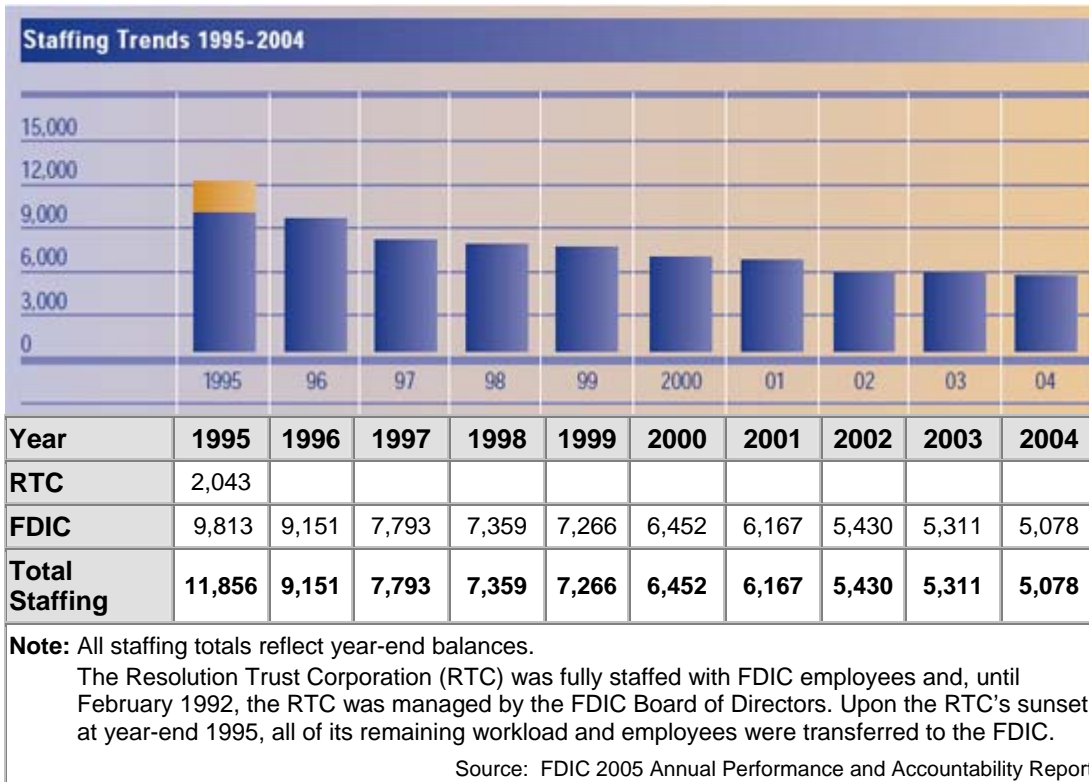
the rest of this decade. A key part of its human capital strategy is the Corporate Employee Program designed to help create a more adaptable permanent workforce and that reflects a more collaborative and corporate approach to meeting critical mission functions. The challenge now is implementing its strategy and monitoring the success of related human capital initiatives and programs. Additionally, developing new leaders and engaging in succession planning pose a challenge. Finally, in

an age of identity theft risks, the FDIC needs to maintain effective controls to protect personal employee-related information that the Corporation possesses. The appointment of a chief privacy officer and implementation of a privacy program are positive steps to address that challenge. Given the importance of the Corporation’s human capital and the critical work of the FDIC, employee integrity is a cornerstone for successful accomplishment of the FDIC mission.

**Potential Outcomes**

- An effective FDIC discrimination complaint resolution system.
- Modern human capital strategies.
- Employee protection from incidents of identity theft or other inappropriate use of personal information.
- Heightened awareness of unacceptable or unethical employee behavior and the appropriate consequences for such behavior.

**Figure 5.3: Corporate Staffing**



## **2006 Performance Goal 5.3:** *Promote maximization of IT resources for efficiency and effectiveness and ensure IT and physical security to protect all FDIC resources from harm.*

### **Key Efforts**

- Assess the FDIC's progress in implementing an enterprise architecture program that supports the FDIC's mission.
- 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.
- Determine whether the FDIC's security controls provide reasonable assurance that its wireless communications and business applications are adequately protected.
- Determine whether the FDIC's security self-assessment and certification and accreditation practices are consistent with federal standards, guidelines, and recognized practices.
- Evaluate the extent of the FDIC's progress in developing and implementing a comprehensive Emergency Preparedness Plan and IT disaster recovery capability.

### **Significance**

The FDIC seeks to maximize its IT resources to improve the efficiency and effectiveness of its operational processes. The Corporation's IT transformation initiative is focusing on three broad areas:

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

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

requirements. The establishment of an integrated and streamlined e-government infrastructure is a key component of the Corporation's target EA. In this connection, the Corporation has initiated a number of major projects designed to improve internal operations, communications, and service to members of the public, business, and other government entities.

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

Additionally, following Y2K and in light of terrorist-related disruptions and, more recently, negative impacts of natural disasters, the importance of corporate disaster recovery and

business continuity planning has been underscored and elevated to an enterprise-wide level. Such planning involves more than the recovery of the technology; it is the recovery of the entire business. The FDIC must be sure that its Emergency

Preparedness Program provides for the safety and physical security of its personnel and ensures that its critical business functions remain operational during any emergency.

### **Potential Outcomes**

- A comprehensive, well-conceived Enterprise Architecture, or blueprint of the agency's current and planned operating systems environment that sets strategic direction for the Corporation's IT investments.
- Strengthened, up-to-date information and system security controls and practices.
- Effective safeguarding of personal information.
- Secure wireless communications and business applications.
- Effective emergency response procedures and a sound business continuity plan.

---

## **2006 Performance Goal 5.4:** *Evaluate the Corporation's contracting efforts to ensure goods and services are fairly, efficiently, and economically procured.*

### **Key Efforts**

- Determine the extent to which the FDIC's performance-based contracts are consistent with FDIC and applicable government-wide guidance and practices.
- Assess the strengths and weaknesses of the FDIC's contract administration policies, procedures, and practices for ensuring contract cost, schedule, and performance requirements are met.
- Determine whether task orders for IT services are being awarded consistent with sound procurement practices.
- Determine whether there are adequate controls to ensure that work performed under the FEDSIM contract for IT support services complies with the terms and conditions of the contract and validate that this contracting method has produced the intended results.
- Determine whether the FDIC is adequately establishing and maintaining contract files to ensure that necessary documents are available to perform and support contract planning, award, and administration activities.
- Determine whether the structure of the Corporation's consolidated facilities management contract (13 facilities-related contracts combined into a single "bundled" contract) and its management of the contract were adequate to ensure the economical and efficient management of the FDIC's Washington, DC facilities.
- For pre-award audits—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.
- For contract billing audits—determine whether contractor billings are allowable under the contract, allocable, and reasonable.

## 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. Many employees with contracting expertise have left the Corporation and contract management responsibilities have shifted. Also, a number of new contracting vehicles and approaches are being implemented. For example, the Corporation combined approximately 40 IT-related

contracts into 1 contract with multiple vendors for a total program value of \$555 million over 10 years. Also, for the first time, it is using a large technical infrastructure contract through the General Services Administration (GSA) valued at over \$300 million. With the expected benefits of these contracts come challenges. The Corporation has not previously outsourced a procurement process to GSA, and both new contracts are performance-based, requiring different oversight mechanisms and strategies than the time and materials contracts that the Corporation has historically used.

## Potential Outcomes

- Improved contracting approaches that save money and ensure optimum performance.
- Strengthened contract administration.
- Enhanced management and operation of all FDIC infrastructure facilities, hardware, software, and systems.
- Reliable, complete system of contract documents to facilitate decision-making, support actions taken, and provide information for reviews, investigations, or litigation.

## 2006 Performance Goal 5.5:

*Monitor corporate efforts to identify and analyze the FDIC risk environment and validate that a sound internal control environment is in place and working well.*

## Key Efforts

- Determine the extent to which the FDIC has implemented its internal control program consistent with applicable government-wide guidance and best practices.
- Internal control component of each audit/evaluation assignment.

## Significance

As an integral part of its stewardship of the insurance funds, the FDIC has established a risk management and internal control program. The Corporation has committed to adopting an Enterprise Risk Management approach to identifying and analyzing risks on an integrated, corporate-wide basis. Revised OMB Circular A-

123, which became effective for fiscal year 2006, requires a strengthened process for conducting management's assessment of the effectiveness of internal control over financial reporting. The circular also emphasizes the need for agencies to integrate and coordinate internal control assessments with other internal control-related

activities and ensure that an appropriate balance exists between the strength of controls and the

relative risk associated with particular programs and operations.

**Potential Outcomes**

- An enterprise-wide control environment that strikes the right balance of internal controls and corporate risks.
- Elimination of control weaknesses.
- Better informed decisions and increased management accountability.





## **Strategic Goal 6: Continuously Enhance the OIG's Business and Management Processes**

The FDIC OIG is one of 57 such offices in the federal government. Along with the Government Accountability Office (GAO) and other law enforcement organizations, the Inspectors General are part of a network of government organizations with common purposes for fostering greater accountability, integrity, and excellence in government programs and operations. Although no two organizations are identical, these organizations provide the FDIC OIG with an opportunity to observe and adopt best practices in use in other organizations with similar missions and values.

While the purpose of our organization is focused on FDIC's programs and operations, the OIG has an inherent obligation to hold itself and its people 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.

**2006 Performance Goals:** To continuously enhance the OIG's business and management processes, the OIG will

- Enhance strategic and annual planning and performance measurement,
- Strengthen human capital management to achieve enhanced results,
- Ensure the quality and efficiency of OIG audits, evaluations, and investigations,
- Foster good relationships with clients, stakeholders, and OIG staff, and
- Invest in cost-effective and secure IT that improves performance and productivity.

---

### **2006 Performance Goal 6.1: *Enhance strategic and annual planning and performance.***

#### **Key Efforts**

- Develop an outcome-oriented strategic and annual plan with performance targets for the OIG.
- Align the contents and timeframes for the strategic plan, management and performance challenges, budget, performance plan, annual audit plan, and the semiannual report.
- Refine our budget process for fiscal year 2008 to incorporate anticipated outcomes and benefits of OIG work.
- 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 is developing a new strategic plan that will add 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

- Continued ability of the OIG to focus on the most important issues facing the FDIC and the Congress on banking and deposit insurance issues.
- Improved 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.
- Clearer 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.



---

**2006 Performance Goal 6.2:**  
*Strengthen human capital management to achieve enhanced results.*

**Key Efforts**

- Develop a training and development program that focuses on the core competencies that OIG managers and staff need to achieve strategic results.
- Manage workforce vacancy opportunities to more fully integrate them with the OIG's strategic goals and objectives and gaps in workforce competencies.
- Develop workforce baseline data to aid in strategic human capital decision-making.
- Mentor selected OIG staff in a pilot internal mentoring program.

**Significance**

To ensure that the OIG has the human resources needed to accomplish its work, it is critical that it align its human capital policies and planning with its strategic and performance goals. Key efforts are focused on integrating workforce planning, training

and development, and hiring and promotion decisions to ensure the OIG attracts, retains, motivates, promotes, and rewards staff with the skills to achieve strategic and annual goals.

**Potential Outcomes**

- Continued alignment of human capital resources with the OIG's strategic goals and objectives.
- Enhanced utilization and productivity of staff.
- An improved training and development program that prepares staff to achieve the OIG's strategic goals.

---

**2006 Performance Goal 6.3:**  
*Ensure the quality and efficiency of OIG audits, evaluations, and investigations.*

**Key Efforts**

- Prepare for an external peer review of the OIG Office of Investigations in fiscal year 2006.
- Prepare for an external peer review of the OIG Office of Audits in fiscal year 2007.
- Plan and conduct an external peer review of the Department of Justice OIG audit function in accordance with the review schedule developed by the President's Council on Integrity and Efficiency (PCIE).
- Review and enhance OIG business process efficiency.

## 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 and evaluation work in accordance with generally accepted *Government Auditing Standards* and its investigations, which often involve allegations of serious wrongdoing that may involve potential violations of criminal law, in accordance with investigation standards 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 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.

---

## ■ **2006 Performance Goal 6.4:** *Foster good relationships with clients, stakeholders, and OIG staff.*

### Key Efforts

- Strengthen 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.
- 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.
- Participate with other OIGs in the PCIE and meet with other accountability and law enforcement organizations.
- 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.

- Increase the accessibility of OIG products.

## 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 IG 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/or Vice Chairman through briefings about ongoing and completed audits, evaluations, and investigations. It also communicates with them and other FDIC officials with a weekly highlights report that provides information of significance about recent audits and ongoing investigations. The OIG is a regular participant in the Audit Committee as recently issued audit 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](http://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 Council

- addresses integrity, economy, and effectiveness issues that transcend individual Government agencies; and
- increases the professionalism and effectiveness of IG 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 appointed OIG staff, meets regularly and provides advice to the Inspector

### 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.

General on a wide variety of issues in a non-threatening environment. A Diversity Coordinator also helps promote corporate diversity initiatives in our workplace.

---

## **2006 Performance Goal 6.5:**

*Invest in cost-effective and secure information technology that improves performance and productivity.*

### Key Efforts

- Enhance the security of OIG information in the FDIC computer network architecture.
- Update OIG information systems to support integrated strategic and annual planning, performance measurement and reporting, and budget formulation and justification.
- Invest in enhanced IT equipment and software when it is cost-effective for improving security, performance, and productivity.

### Significance

Information Technology 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 Division of Information Technology, the OIG will strengthen and enhance security and operational controls over network equipment and procedures to protect OIG information better.

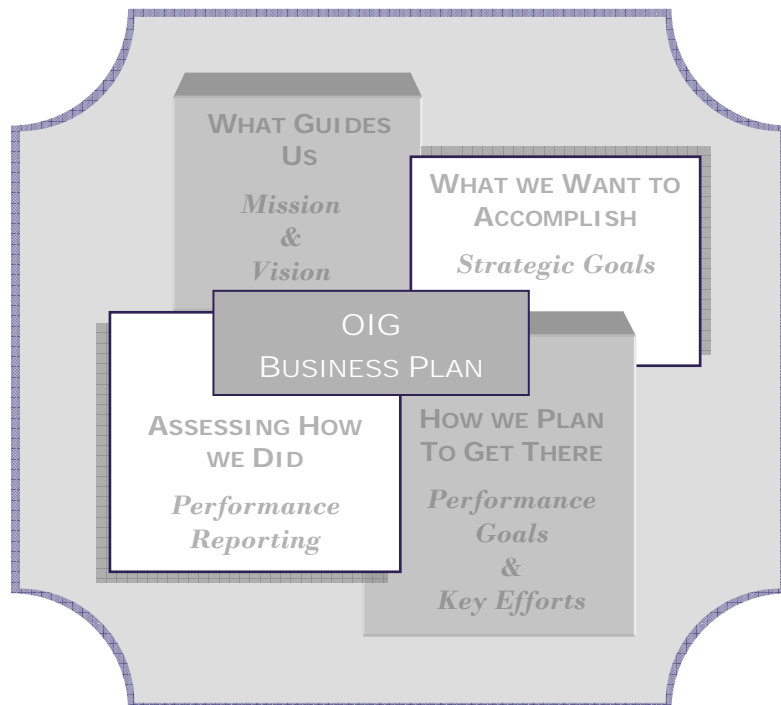
The OIG also develops and maintains information systems that track the status of ongoing audits, evaluations, and investigations to help ensure the timeliness of our work and monitor our

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 2006 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 2003 Actual	FY 2004 Actual	FY 2005 Actual	FY 2006 Target
Financial Benefit Return <sup>a</sup>	377%	360%	155%	100%
Other Benefits <sup>b</sup>	N/A	N/A	N/A	70
Past Recommendations Implemented <sup>c</sup>	N/A	N/A	92%	95%
Audit/Evaluation Reports Issued	47	48	40	30
Average Elapsed Calendar Days to Issue Final Audit/Evaluation Report	223	189	225	180
Investigation Actions <sup>d</sup>	160	98	130	120
Closed Investigations Resulting in Reports to Management, Convictions, Civil Actions, or Administrative Actions	70%	81%	82%	80%
Investigations Accepted for Prosecution Resulting in Convictions, Pleas, and/or Settlements	76%	70%	80%	70%
Investigation Reports Issued Within 30 Days After Completing Case	100%	100%	100%	100%

<sup>a</sup> 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.

<sup>b</sup> 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.

<sup>c</sup> Fiscal year 2004 recommendations implemented by fiscal year-end 2006.

<sup>d</sup> Indictments, convictions, informations, arrests, pre-trial diversions, criminal non-monetary sentencings, monetary actions, employee actions, and other administrative actions.

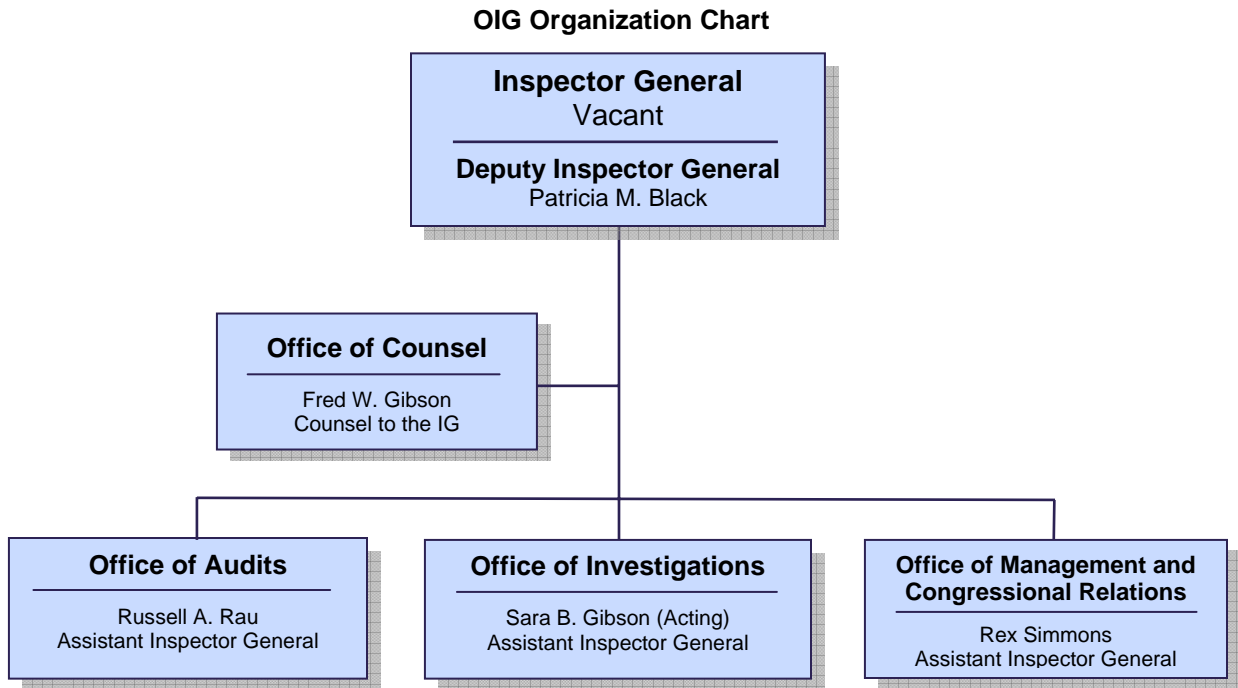
---

# APPENDIX I

---

## *OIG Organization Structure*

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



---

### *Office of Audits*

The Office of Audits performs a wide range of professional audits and evaluations of nationwide FDIC corporate and banking industry activities. 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. The Office of Audits is also charged with quickly evaluating and recommending improvements to FDIC operations. Audits and evaluations often focus on special requests received from senior FDIC managers and the OIG Hotline. The OIG will also initiate assignments in areas

where there is potential to improve program performance by providing analyses and recommendations on critical, time-sensitive issues confronting the FDIC.

The Office of Audits is organized into three primary Directorates: (1) Insurance, Supervision, and Receivership Management Audits; (2) Systems Management and Security Audits; and (3) Corporate Evaluations and Audits. Each Directorate is responsible for addressing significant risks and challenges facing the Corporation.

## *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 allegations of fraud, waste, abuse, and mismanagement 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 information technology

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 2006 budgetary resources (based on projected spending for the year) and the associated human capital resources in terms of full-time equivalent (FTE) positions by strategic goal.

**FY 2006 Resources by Strategic Goal**

Strategic Goal	Amount	Percent	FTEs	Percent
<b>Strategic Goal 1:</b> Assist the FDIC to Ensure the Nation's Banks Operate Safely and Soundly	\$11,800,000	45%	63	47%
<b>Strategic Goal 2:</b> Help the FDIC Maintain the Viability of the Insurance Funds	\$1,500,000	6%	8	6%
<b>Strategic Goal 3:</b> Assist the FDIC to Protect Consumer Rights and Ensure Community Reinvestment	\$2,450,000	9%	13	10%
<b>Strategic Goal 4:</b> Help Ensure that the FDIC is Ready to Resolve Failed Banks and Effectively Manages Receiverships	\$1,200,000	5%	6	5%
<b>Strategic Goal 5:</b> Promote Sound Governance and Effective Stewardship of Financial, Human, IT, and Procurement Resources	\$7,200,000	28%	33	25%
<b>Strategic Goal 6:</b> Continuously Enhance the OIG's Business and Management Processes	\$1,850,000	7%	10	7%
<b>Total</b>	<b>\$26,000,000</b>	<b>100%</b>	<b>133</b>	<b>100%</b>

---

## 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.

<b>External Factor</b>	<b>Description</b>
<b>Budget</b>	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. For FY 2006, the Congress appropriated \$30.7 million (including a 1-percent rescission), which is about \$800,000 more than the OIG requested.
<b>External Requests</b>	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.
<b>Number of Bank Failures</b>	In the last few years, the economy has been strong and banks have prospered. In 2005, for the first time in the FDIC's history, no banks have failed. 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.
<b>Emerging Technology</b>	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.
<b>Changes in Financial Services Industry</b>	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 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
<b>Management and Performance Challenges</b>	<p>In the spirit of the Reports and 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.</p> <ul style="list-style-type: none"> <li>▪ Assessing and mitigating risks to the insurance funds;</li> <li>▪ Ensuring institution safety and soundness through effective examinations, enforcement, and follow-up;</li> <li>▪ Contributing to public confidence in insured depository institutions;</li> <li>▪ Protecting and educating consumers and ensuring compliance;</li> <li>▪ Being ready for potential institution failures; and</li> <li>▪ Managing and protecting financial, human, information technology, and procurement resources.</li> </ul>
<b>Audit Assignment Plan</b>	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.
<b>External Client Survey</b>	Survey conducted in 2005 of senior FDIC executives and managers to assess their views of the OIG.
<b>OIG Employee Survey</b>	Survey conducted in 2004 of OIG employees' views about their work environment.
<b>OIG Human Capital Strategic Plan</b>	Identifies strategies for aligning human resources policies and procedures to support the OIG mission.
<b>OIG Training Study</b>	Study analyzing FY 2003 OIG training.
<b>OIG Information Technology Strategic Plan</b>	Sets forth challenges and strategies for the OIG's information technology needs for fiscal years 2005-2007.
<b>Workload and Staffing Analysis</b>	An analysis of OIG 2005 workload and staffing requirements.
<b>Internal Quality Assurance Reviews</b>	Reviews conducted by the OIG of our internal operations.
<b>External Peer Reviews</b>	Evaluation conducted of the OIG's audit operations by the Department of Energy OIG in 2003-2004.
<b>Internal Control Reviews</b>	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.

<b>Data Source</b>	<b>Description</b>
<b>System for Tracking Audits and Reports (STAR)</b>	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.
<b>Investigations Database System (IDS)</b>	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.
<b>OIG Strategic Information Dashboard System</b>	The Dashboard is an executive information system designed to improve the efficiency of OIG management oversight of internal operations. It provides OIG executives with up-to-date information on key OIG performance indicators, the budget and monthly spending reports, staffing, and annual performance goals. The Dashboard also facilitates the reporting and consolidation of status information on the OIG's strategic and annual performance goals.

**Office of Inspector General  
2006 Business Plan**

The Office of Inspector General's  
Strategic Plan and  
FY 2006 Performance Plan

**Federal Deposit Insurance Corporation**

February 2006