



Office of Inspector General

Office of Audits Assignment Plan

Fiscal Year 2006

October 1, 2005 – September 30, 2006



DATE: October 21, 2005

MEMORANDUM TO: Chairman
Board of Directors
Audit Committee
Deputies to the Chairman
Division and Office Directors



FROM: Patricia M. Black
Deputy Inspector General

SUBJECT: Office of Audits Assignment Plan for Fiscal Year 2006

The Federal Deposit Insurance Corporation (FDIC) is an independent agency created by the Congress in 1933 to maintain stability and confidence in the Nation's financial system by insuring deposits, examining and supervising financial institutions, and managing receiverships. The FDIC's Office of Inspector General (OIG) is an independent and objective unit established under the Inspector General Act of 1978, as amended, with the statutory mission of, among other things:

- conducting, supervising, and coordinating audits, evaluations, and investigations relating to the programs and operations of the FDIC;
- providing leadership for activities designed to promote economy, efficiency, and effectiveness, and to promote efforts to reduce fraud, waste, and abuse in corporate programs and operations; and
- informing the Chairman and Congress of problems in FDIC programs and operations and the necessity for and progress of corrective actions.

As a tool in fulfilling these responsibilities, the OIG's Office of Audits prepares an annual assignment plan outlining its planned audit and evaluation coverage for the coming year. This assignment plan covers fiscal year 2006, or the period October 1, 2005 through September 30, 2006.

The assignments included in our fiscal year 2006 Assignment Plan are designed to add value to the Corporation in a variety of ways, including assessing program effectiveness, management, and results; economy and efficiency; internal control; and compliance with legal or other requirements and by helping to deter and detect instances of fraud, waste, and abuse. The assignments entail a variety of methodologies and objectives and will provide findings, analyses, information, and recommendations to help the Corporation achieve its mission. Further, these assignments are intended to provide coverage of the

FDIC's most critical programs and activities and to help the Corporation successfully address risks, meet its challenges, and accomplish its goals and objectives. Finally, in keeping with the intent of the IG Act, our audits and evaluations are a key oversight mechanism for the Congress and the public.

Earlier this year, OIG executives assessed their offices' workload, staffing levels and structures to determine whether changes would be appropriate in the near future. Following that assessment, the OIG developed and implemented a plan for reducing the size of the office consistent with our expected workload. The plan reflected the OIG's assessment of its mission, the risks to the FDIC, and related priorities. As part of that initiative, the Office of Audits has taken steps to reduce its staffing by approximately 30 percent and consolidated its prior six directorates into three:

- Insurance, Supervision, and Receivership Management Audits
- Systems Management and Security Audits
- Corporate Evaluations and Audits

This organization structure is designed to complement the Corporation's principal operational areas. While the reduced resources will result in fewer audits and evaluations, our goal is to add the same level of value and oversight through careful planning and increased efficiency and effectiveness in our processes.

The input we received from corporate management and members of the FDIC Audit Committee in formulating our plan has been useful. The dialogue with FDIC executives and managers, together with an increased emphasis within our own organization on planning and addressing risk, has been helpful in identifying those areas where the OIG can devote resources in the best interest of the Corporation. Our planning process is ongoing and dynamic, and we may alter the focus, timing, and selection of assignments to better respond to legislatively mandated priorities, congressional requests, emerging issues, FDIC corporate governance issues, and changing priorities within the FDIC.

We are committed to working cooperatively with FDIC management and being responsive to the Congress in conducting our audits and evaluations during fiscal year 2006.

TABLE OF CONTENTS

OVERVIEW	1
LIST OF ACRONYMS	2
FDIC OIG ASSIGNMENT PLANNING FRAMEWORK	3
OIG VALUE-ADDED PROCESS	4
INSURED DEPOSITORS ARE PROTECTED FROM LOSS WITHOUT RECOURSE TO TAXPAYER FUNDING	5
FDIC-SUPERVISED INSTITUTIONS ARE SAFE AND SOUND	7
CONSUMERS' RIGHTS ARE PROTECTED AND FDIC-SUPERVISED INSTITUTIONS INVEST IN THEIR COMMUNITIES	11
RECOVERY TO CREDITORS OF RECEIVERSHIPS IS ACHIEVED	13
STRATEGIC RESOURCES ARE EFFECTIVELY MANAGED	
Financial Resources	14
Human Capital	17
Information Technology	18
Business Continuity Planning	21
Enterprise Risk Management	22
OTHER PLANNED ASSIGNMENT	23
APPENDIX I: ONGOING ASSIGNMENTS	24
APPENDIX II: ASSIGNMENTS BY DIRECTORATE	27
APPENDIX III: ASSIGNMENTS BY STRATEGIC AREAS OF FOCUS	29

Overview

The Office of Inspector General (OIG) is a key component of the Federal Deposit Insurance Corporation's (FDIC) risk management program. Our fiscal year 2006 *Office of Audits Assignment Plan* is part of an overall strategy of the OIG to consider current and emerging corporate programs, operations, risks, and management challenges in planning for and budgeting our resources.

The OIG's value-added process, which is depicted on page 4, includes many considerations that impact our determination of the assignments for fiscal year 2006. The process is intended to culminate in our producing results that will enhance FDIC corporate governance and contribute to the Corporation's overall risk management activities.

All of the assignments in our plan will be conducted in accordance with Government Auditing Standards. We organized the assignments by the FDIC's strategic goals, which are to ensure that:

- Insured depositors are protected from loss without recourse to taxpayer funding;
- FDIC-supervised institutions are safe and sound;
- Consumers' rights are protected, and FDIC-supervised institutions invest in their communities;
- Recovery to creditors of receiverships is achieved; and
- Strategic resources are effectively managed.

The Assignment Plan lists and briefly describes each of the 33 assignments that we plan to start in fiscal year 2006, including the objective, background information associated with the area being covered, relevant prior audit coverage, and known risks. Additionally, we have provided:

- a listing of ongoing assignments along with the stated objectives in Appendix I.
- the planned assignments by Office of Audits directorate and a point of contact in Appendix II.

Finally, the OIG is in the midst of revising and enhancing its office-wide risk assessment and planning process. In that regard, we have identified strategic areas of focus that are driven by the Corporation's mission and strategic goals, and going forward, we will be planning our work and aligning our resources within that framework. To that end, we have provided a listing of our fiscal year 2006 assignments by strategic area of focus in Appendix III.

In the spirit of the Reports Consolidation Act of 2000, and as part of our risk assessment process, the OIG will be assessing and identifying what we consider to be the most significant management and performance challenges facing the FDIC. The resulting management and performance challenges will be provided to FDIC for inclusion in their performance and accountability report.

LIST OF ACRONYMS

BCP	Business Continuity Plan
BSA	Bank Secrecy Act
CRA	Community Reinvestment Act
CTR	Currency Transaction Report
DIT	Division of Information Technology
DRR	Division of Resolutions and Receiverships
DSC	Division of Supervision and Consumer Protection
EA	Enterprise Architecture
ECOA	Equal Credit Opportunity Act
ERP	Emergency Response Plan
FDIC	Federal Deposit Insurance Corporation
FDICIA	Federal Deposit Insurance Corporation Improvement Act
FEDSIM	Federal Systems Integration Management
FinCEN	Financial Crimes Enforcement Network
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
GAS	Government Auditing Standards
GPRA	Government Performance and Results Act
GSA	General Services Administration
HMDA	Home Mortgage Disclosure Act
IT	Information Technology
MLR	Material Loss Review
NCRC	National Community Reinvestment Coalition
NFE	New Financial Environment
OERM	Office of Enterprise Risk Management
OIG	Office of Inspector General
OMB	Office of Management and Budget
RUP [®]	Rational Unified Process
SAR	Suspicious Activity Reports
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act



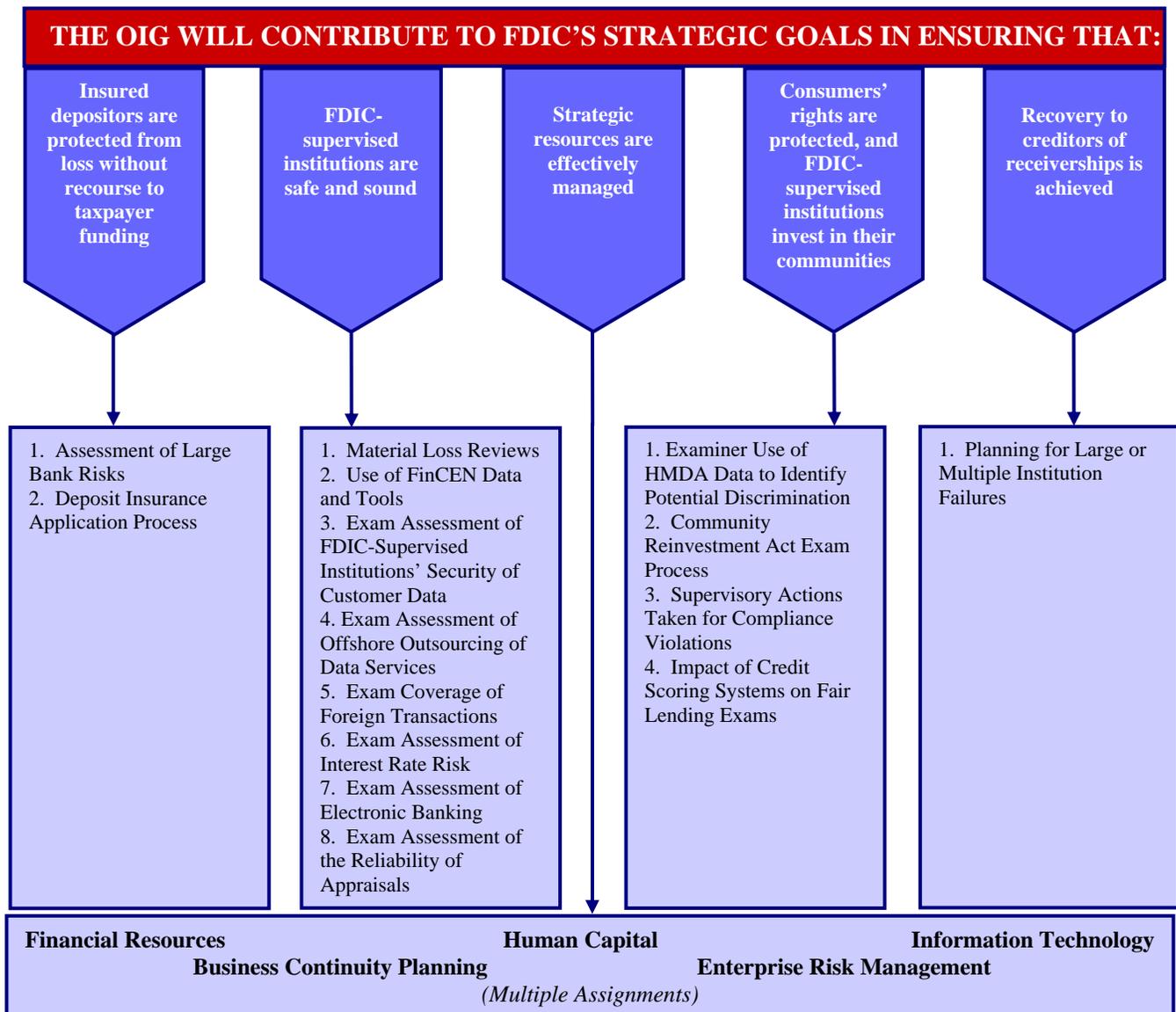
FDIC OIG ASSIGNMENT PLANNING FRAMEWORK

OIG MISSION

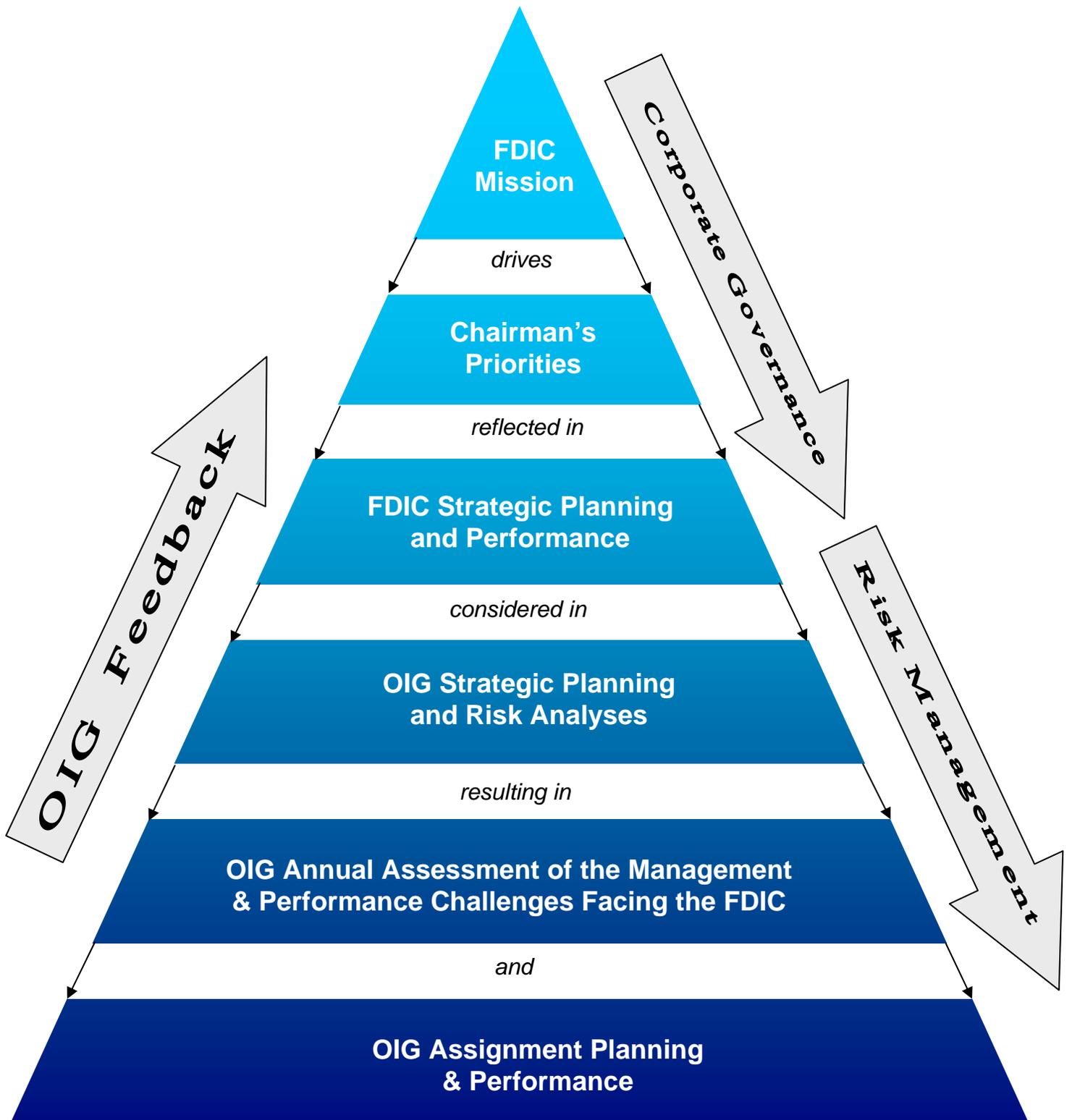
- Promote the economy, efficiency, and effectiveness of FDIC programs and operations.
- Protect against fraud, waste, and abuse.
- Assist and augment the FDIC’s contribution to the stability of, and public confidence in, the Nation’s financial system.

OIG STRATEGIC GOAL (Value and Impact)

OIG products will add value by achieving significant impact related to addressing issues of importance to the FDIC, the Congress, and the public.



OIG VALUE-ADDED PROCESS



Insured Depositors Are Protected From Loss Without Recourse to Taxpayer Funding

Deposit insurance is a fundamental part of the FDIC's commitment to maintain stability and public confidence in the U.S. financial system. As of the end of the second quarter of 2005, the FDIC insured \$3.757 trillion in deposits for 8,881 institutions. When insured depository institutions fail, the FDIC ensures that financial institution customers have timely access to their deposits and other services. To ensure that depositors are protected from loss, the deposit insurance funds must remain viable so that adequate funds are available in the event of an institution's failure. The FDIC maintains sufficient deposit insurance fund balances by collecting risk-based insurance premiums from insured depository institutions and through its own fund investment strategies. The FDIC continually evaluates the adequacy of the deposit insurance funds. It identifies risks to the insurance funds by analyzing regional, national, and global economic, financial, and financial institution developments, and by collecting and evaluating information through the supervisory process.

1. Assessment of Large Bank Risks

The FDIC has reported that the increased complexity of the industry and the concentration of risk to the insurance funds in the largest banking organizations are expected to grow more pronounced over time and to present greater risk-management challenges to the Corporation. As insurer, the FDIC needs a good understanding of the risks that the largest institutions pose to the funds. As of June 30, 2005, the 25 largest banks controlled \$5.64 trillion (54 percent) of total bank assets in the country. The FDIC is the primary federal regulatory for only 2 of these 25 financial institutions. The FDIC established the Large Bank Section in the Division of Supervision and Consumer Protection (DSC) to identify, analyze, and monitor risks to the deposit insurance funds posed by the largest and most complex institutions. Key supervisory programs administered by this section include:

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

In addition, the FDIC established the Resolutions Policy Committee to ensure that 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 objective is to develop a strategy for audit coverage of the FDIC's approach to assessing and addressing risk posed to the insurance funds by large banks. We envision a series of audits that will address the Corporation's key programs and activities in this area.

2. Deposit Insurance Application Process

The FDIC is solely authorized to approve applications for deposit insurance under section 115 of the Federal Deposit Insurance Corporation Improvement Act. In evaluating and approving applications for deposit insurance, Section 6 of the Federal Deposit Insurance Act of 1991 (FDICIA) requires the FDIC to consider certain statutory factors, including the risk the institution poses to the insurance funds. Implicit in the favorable resolution of the applicable statutory factors for most applications processed is the consideration of a financial institution's compliance with Bank Secrecy Act (BSA) and anti-money laundering requirements. In addition, proposals involving institutions, including certain industrial loan companies and credit card banks, that are to be owned by or significantly involved in transactions with commercial or financial companies, present unique characteristics that may warrant the imposition of prudential conditions. These recommended conditions are intended to achieve a standard for prudent operation that is expected of all insured institutions. The FDIC's deposit insurance application review process is the first step in managing risks to the deposit insurance funds.

The objective is to evaluate the FDIC's process for reviewing and investigating applications for deposit insurance and determine whether the process, when implemented, fully considers statutory and other applicable factors.

FDIC-Supervised Institutions Are Safe and Sound

As insurer, the FDIC is concerned with the safety and soundness of all insured institutions. However, a distinction is made between the FDIC's role as an insurer and its role as the primary federal regulator for state non-member banks. As of September 30, 2005, the FDIC was the primary supervisor for 5,257 financial institutions. In that capacity, the FDIC conducts examinations to assess the operating condition, management practices and policies of the institutions; prepares and issues rules and regulations that govern the business and activities of the institutions in a wide range of areas; and provides guidance for the safe, sound, and prudent operation of these institutions and related entities. The FDIC also reviews applications submitted by FDIC-supervised institutions to expand their activities or locations. When appropriate, the FDIC has a range of informal and formal enforcement options available to resolve problems identified at FDIC-insured institutions.

1. Material Loss Reviews

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

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

2. Use of FinCEN Data and Tools

Although the Treasury Department has overall authority for BSA enforcement and compliance, the Financial Crimes Enforcement Network (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. Two prior OIG audits focused on other aspects of BSA compliance. Specifically, one audit focused on the FDIC's process for ensuring corrective

actions were taken by bank management to address BSA violations, and the other audit focused on an institution's compliance with BSA.

The audit objective is to determine whether the FDIC is adequately using FinCEN data and tools in assessing the BSA and anti-money laundering programs of FDIC-supervised financial institutions.

3. Examination Assessment of FDIC-Supervised Institutions' Security of Customer Data

The explosive growth of the Internet and the development of sophisticated computer systems and databases have made it easier for companies, including financial institutions, to gather and use information about their customers. Despite generally strong controls and practices by financial institutions, methods for obtaining unauthorized access to personal data and misusing that data are continuously evolving. Identity theft is one of the fastest growing types of consumer fraud. As recent security breaches demonstrate, if this information is not adequately secured, it can fall into the wrong hands and cause serious harm to consumers. In its role as supervisor, the FDIC must stay abreast of the serious weaknesses that can threaten both the security of the stored data and the vulnerability of the systems themselves. The FDIC's risk-focused information technology (IT) examination procedures focus on the financial institution's information security program and risk-management practices for securing information assets, including controls designed to protect information from intentional or inadvertent disclosure to unauthorized individuals.

The audit objective is to determine the extent to which the FDIC's information technology examinations ensure that FDIC-supervised institutions are adequately protecting customer data.

4. Examination Assessment of Offshore Outsourcing of Data Services

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

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

The FDIC assesses the risks related to offshoring as part of its IT examination process.

The audit objective is to determine whether FDIC examinations are effectively assessing the data security risks associated with offshore outsourcing.

5. Examination Coverage of Foreign Transactions

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) (Public L. No. 107-560), enacted on October 26, 2001, made a number of amendments to the anti-money laundering provisions of the BSA. As required by statute, the Treasury Department amended its Financial Recordkeeping and Reporting of Currency and Foreign Transactions rules. The amendments were intended to make it easier to prevent, detect, and prosecute money laundering and the financing of terrorism. Likewise, the FDIC revised its examination procedures for assessing the anti-money laundering programs to incorporate new regulations. Specifically, in June 2005, the FDIC, in conjunction with the other federal banking regulators, issued revisions to its BSA examination procedures. These examination procedures will be used to assess financial institutions' routine anti-money laundering and risk-management practices to ensure that banks do not unwittingly become involved in money laundering schemes conducted by foreign officials, their immediate family members, or their close associates.

The audit objectives are to determine the extent to which FDIC examiners are following BSA examination procedures for foreign transactions.

6. Examination Assessment of Interest Rate Risk

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

The audit objectives are to (1) determine whether the FDIC's examinations comply with applicable policies and procedures for assessing and addressing institutions' sensitivity to

interest rate changes and (2) assess the contributions of other related corporate activities to the examination assessment of interest rate risk.

7. Examination Assessment of Electronic Banking

Financial institutions are becoming more aggressive in adopting electronic banking (e-banking) capabilities that include sophisticated marketing systems, remote banking capabilities, and stored value programs. These emerging technologies yield a variety of delivery options and innovative products and services, but also present opportunities as well as risks to an insured financial institution. As part of its IT examination process, the FDIC must consider:

- Security controls for safeguarding customer information.
- Authentication processes necessary to verify the identity of customers.
- Liability for unauthorized transactions.
- Losses from fraud if the institution fails to verify the identify of individuals or businesses applying for new accounts or credit on-line.
- Possible violations of laws or regulations pertaining to consumer privacy, anti-money laundering, anti-terrorism, or the content, timing, or delivery of required consumer disclosures.
- Negative public perception, customer dissatisfaction, and potential liability resulting from the failure to process third-party payments as directed, lack of availability of on-line services, or unauthorized access to confidential customer information.

The FDIC's assessment of e-banking risk in a financial institution should also take into account the network environment, the security of internal networks, and the security of public networks commensurate with the bank's operational complexity and sophistication.

The audit objectives are to determine (1) whether the FDIC's examination procedures address the risks associated with electronic banking and (2) the extent to which examiners are following those procedures.

8. Examination Assessment of the Reliability of Appraisals

The degree of risk in a real estate loan depends primarily on the loan amount in relation to the collateral value, the interest rate, and most importantly the borrower's ability to repay. Appraisals are professional judgments of the market value of real property and are one of the essential components of the lending process. For the purpose of collateral administration in a loan portfolio, an institution's estimate of value of real property may be supported by an existing or new appraisal or evaluation. The bank's adherence to the appraisal regulations and appraisal guidelines should be part of the examiner's overall review of the lending function to help ensure that there is sufficient collateral to protect the bank in case of foreclosure.

The audit objective is to determine whether the FDIC's examinations adequately assess the reliability of appraisals as part of the evaluation of an institution's lending policies and practices.

Consumers' Rights Are Protected and FDIC-Supervised Institutions Invest in Their Communities

The FDIC promotes institution compliance with consumer protection and fair lending laws. The FDIC engages in a variety of activities related to consumer protection and fair lending, including: (1) providing consumers with access to easily understood information about their rights and the disclosures due them under consumer protection and fair lending laws; and (2) examining FDIC-supervised institutions to determine their compliance with consumer protection and fair lending laws and evaluating their performance under the Community Reinvestment Act of 1977 (CRA). In addition, the FDIC educates bankers and consumers on matters of interest and addresses consumers' questions and concerns.

1. Examiner Use of HMDA Data to Identify Potential Discrimination

Housing loans covered by the Home Mortgage Disclosure Act (HMDA) include home purchase, home improvement, and refinance loans for single family dwellings (1 to 4 units) and loans for multi-family units. The number of applications for these loans has substantially increased, and the likelihood of potential discrimination may increase proportionately. Widespread reports of predatory lending practices, including price discrimination, threatens the possibility of creating sustainable and affordable homeownership opportunities for residents of traditionally underserved neighborhoods. A study performed by the National Community Reinvestment Coalition (NCRC) in 2003 found that African-American and predominantly elderly communities receive a considerably higher level of high-cost subprime loans than is justified based on the credit risk of neighborhood residents. During 2004, lenders started collecting for the first time, and will report by March 1, 2005, information for "higher-priced" loans by the income level of the census tract in which the property is located and by borrower characteristics (income, race, ethnicity, and gender). A loan is "higher-priced" and covered by these reporting requirements only if the spread between the annual percentage rate on the loan and the yield on comparable Treasury securities is greater than 3 percentage points for first-lien loans, or 5 percentage points or more for subordinate-lien loans. The information may help detect predatory or abusive lending as well as discriminatory pricing.

The audit objective is to 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.

2. Community Reinvestment Act Examination Process

In 1977, the Congress 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 regulatory agencies 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. The FDIC, Federal Reserve, and Office of the Comptroller of the Currency jointly approved

amendments to the CRA regulations, effective September 1, 2005, that provide regulatory relief for smaller community banks and preserve the importance of community development in the CRA evaluations of these banks.

The audit objectives are to (1) 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 (2) assess how the FDIC is measuring and reporting on the effectiveness of the new procedures.

3. Supervisory Actions Taken for Compliance Violations

The FDIC enforces compliance with fair lending, privacy, and various other consumer protection laws and regulations, primarily through compliance examinations. It is important that consumers and businesses obtain the benefits and protection afforded them by law. The compliance examination and follow-up supervisory attention accorded to violations and other deficiencies helps to assure this result. The presence of violations and the absence of an effective program to manage a financial institution's compliance responsibilities reflect adversely on senior management and the board of directors and may carry over into other areas of management responsibility. Additionally, DSC considers compliance with fair lending, privacy, and other consumer protection requirements when reviewing an application for entry into or expansion within the insured depository institution system. Prior OIG audit work in this area focused on DSC's risk-focused compliance examination procedures.

The audit objective is to determine whether the FDIC adequately addresses the violations and deficiencies reported in compliance examinations to ensure that FDIC-supervised institutions take appropriate corrective action.

4. Impact of Credit Scoring Systems on Fair Lending Examinations

The Equal Credit Opportunity Act (ECOA) applies to all creditors and promotes the availability of credit to all creditworthy applicants. Specifically, ECOA prohibits creditor practices that discriminate on the basis of race, color, religion, national origin, sex, marital status, or age. Credit scoring is a system used to evaluate an applicant's creditworthiness, based on the key attributes of the applicant and aspects of the transaction. Scoring models are analytical tools designed to provide portfolio managers with the ability to statistically quantify risk. A failure of credit scoring models to consider information relating to the economic and personal circumstances of individuals raises important issues that may affect the ability of the scoring systems to accurately quantify the credit risk of individuals.

The audit objective is to evaluate the FDIC's approach to fair lending examinations when a financial institution uses credit scoring systems.

Recovery to Creditors of Receiverships Is Achieved

When an institution fails, the FDIC is appointed receiver and assumes responsibility to recover, as quickly as it can, the maximum amount possible on the receivership's claims. Having fulfilled its obligations as deposit insurer, the FDIC is often the largest creditor. The receiver may have valid claims against former directors, officers, attorneys, accountants, or other professionals who may have caused harm to the institution. Funds collected through the pursuit of valid claims and the sale of assets are distributed to the creditors according to priorities set by law. Once the FDIC sells the receivership's assets and resolves its obligations, claims, and any legal impediments, the receivership is terminated and a final distribution is made to its creditors.

1. Planning for Large or Multiple Institution Failures

The mission of the Division of Resolutions and Receiverships (DRR) is to plan for and efficiently handle the resolutions of failing FDIC-insured depository institutions and to provide prompt, responsive, and efficient administration of failing and failed FDIC-insured institutions in order to maintain confidence and stability in the Nation's financial system. Part of DRR's responsibility is to ensure that bank customers have timely access to their insured deposits at failed insured depository institutions either by facilitating the transfer of their insured deposits to an assuming institution or by paying insured depositors directly. Planning models for responsiveness to failing and failed institutions, including large or multiple bank failures, need to be evaluated, revisited, and tested for adequacy in light of the impact of recent corporate and external events. These events include: FDIC downsizing activities; the continued threat of terrorist-related activities; and natural disasters that change the operating environment in which FDIC resources must react.

The audit objective is to assess the effectiveness of the FDIC's planning for large or multiple bank failures.

Strategic Resources Are Effectively Managed

Properly managing and utilizing critical financial, human, and information technology resources is necessary to enable the FDIC to carry out its mission successfully. Effective management involves protecting these resources through sound stewardship, procurement, and security practices. The FDIC's support divisions and offices play a key role in managing strategic resources. Further, the FDIC has embarked upon enterprise-wide business continuity planning which involves more than the recovery of technology, and has defined it as the recovery of the business regardless of the nature of the disruption. The FDIC has developed an Emergency Preparedness Program that provides for the safety and security of its personnel through the Emergency Response Plan (ERP) and ensures that its critical business functions remain operational during any emergency. In addition, the Corporation has sought to enhance its internal control program by adopting an enterprise risk-management focus.

Financial Resources

1. Performance-based Contracting

The Government Accountability Office (GAO) report entitled, *Federal Procurement: Spending and Workforce Trends* (GAO-03-443), indicates that significant growth in service contracts has led the Congress and the Administration to encourage greater use of performance-based service contracting to achieve greater cost savings and better outcomes. Under performance-based approaches, the contracting organization specifies the outcome or desired results and lets the contractor decide how best to achieve the desired outcome. The GAO report indicates that agencies may not have an adequate understanding of performance-based contracting and how to take full advantage of this approach. In addition, GAO reported that agency officials have acknowledged the need for better guidance on performance-based contracting and better criteria for identifying which contracts should be called "performance based." The Office of Federal Procurement Policy is developing guidance to help agencies improve their use of performance-based contracting. The FDIC has awarded a few performance-based contracts, but is still exploring how and when to use these types of contracts. A prior OIG audit related to one such contract found that the contract incentives could have been strengthened to improve contractor performance and better manage costs.

The audit objective is to determine the extent to which the FDIC's performance-based contracts are consistent with FDIC and applicable government-wide guidance and practices.

2. Contract Administration

Contract administration begins after the contract has been awarded, and ends when the goods or services have been accepted and the contractor has received final payment. The contractor's progress must be closely monitored to identify potential problems that threaten performance. Contract administration includes the efforts of FDIC oversight managers and technical monitors. Adequate contract administration ensures that the contractor delivers the required goods or performs the work according to the delivery schedule in the contract. It also includes monitoring cost, schedule, and technical performance and ensuring that payments are properly authorized and supported. The Corporation's exposure to risk is greater with increased reliance on outsourcing, if those contracts are not properly managed. Maintaining strong internal controls and effective oversight of contracting activities is critical to the FDIC's success, and the FDIC is continuing to work on improving its contract-management practices. This assignment will complement prior OIG audit work that focused on other aspects of the FDIC's procurement process including acquisition planning and execution strategy and contract solicitation and evaluation processes.

The audit objective is to assess the strengths and weaknesses of the FDIC's contract administration policies, procedures, and practices for ensuring that contract cost, schedule, and performance requirements are met.

3. Classifying Salary Costs in the NFE

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

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

4. Information Technology Application Services Task Order Awards

The FDIC, through the General Services Administration's (GSA) FedBizOpps Electronic Posting System, solicited and selected several contractors to perform a wide range of IT services. The Information Technology Application Services contract combined

approximately 40 contracts into 1 contract with multiple vendors for a total program value of \$555 million over 10 years. In such a large contractual undertaking, significant risk may exist in getting the work completed and in overseeing the large task orders. Further, the actual task order award methodology and the level of detail in the descriptions of work are key to the FDIC avoiding protests and receiving needed goods and services at fair and reasonable prices.

The audit objective is to determine whether Information Technology Application Services task orders are being awarded consistent with sound procurement practices.

5. Interagency Agreement with GSA Under the FEDSIM Contract

In March 2004, the FDIC entered into an interagency agreement with GSA -- the Federal Systems Integration Management (FEDSIM) contract (04-00125-T-DY) -- to provide assistance for IT support services. The performance-based contract provides for managing and operating all FDIC infrastructure facilities, hardware, software, and systems to include, but not limited to, help desk operations, network operations management, data center support, technology deployment support, test lab support, and security operations. As of June 2005, a Contract Monitoring Information Application report indicated that the FEDSIM contract totaled \$342 million. Considering the significant contract cost and the vital IT functions that are being acquired, the success of the FEDSIM contract will be extremely important to the FDIC for many years to come. While conducting this audit, we will coordinate with the GSA OIG, although that office has advised us that they expect audit coverage of such contracts to be provided by the client agency.

The audit objectives are to determine whether (1) there are adequate controls to ensure that work performed under the FEDSIM contract complies with the terms and conditions of the contract and (2) this contracting method has produced the intended results.

6. Contract File Management

The content and organization of contract files is essential to the effectiveness of contract planning, award, and administration efforts. Contract file documentation should be sufficient to constitute a complete history of the contract for the purpose of:

- providing a complete background as a basis for informed decisions at each step in the acquisition process,
- supporting actions taken,
- providing information for reviews and investigations, and
- furnishing essential facts in the event of litigation.

Other benefits of a complete and well-organized contract file include:

- deficient contractor performance can be identified and corrected,
- out-of-scope contract work will not be performed inadvertently,
- adverse delivery schedule delays can be minimized or prevented,

- contract billing errors can be detected and related payments can be recovered, and
- contract closeout activities can be completed expeditiously.

Prior OIG reviews have found that contract file documentation is not always complete. Further, the OIG and Division of Administration (DOA) have expressed concerns regarding the data quality and completeness of the FDIC's new Web-based repository for electronically organizing and storing contractual documents.

The audit objective is to 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.

7. Contractor Reviews and Audits

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

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

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

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

Human Capital

1. Succession Planning Efforts

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

of succession planning and management strategies. Prior OIG evaluations have focused on other aspects of the FDIC's human capital program including its overall human capital framework, workforce planning, and the Corporate University.

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

Information Technology

1. The FDIC's Information Security Program--2006

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

The audit objective is to evaluate the effectiveness of the FDIC's information security program and practices, including the FDIC's compliance with FISMA and related information security policies, procedures, standards, and guidelines. As part of our evaluation, we will assess the FDIC's efforts to improve its information security controls and practices relative to the baseline controls covered in our 2005 FISMA report and a new framework based on more recent government-wide guidance.

2. The FDIC's Compliance With Section 522 of the Consolidated Appropriations Act of 2005

On December 8, 2004, the President signed into law H.R. 4818, *Consolidated Appropriations Act, 2005* (Public Law 108-447). Title V, Section 522, of this act mandates the designation of a senior privacy official, establishment of privacy and data protection procedures, a written report of the agency's use of information in an identifiable form, an independent third-party review of the agency's use of information in an identifiable form, and a report by the Inspector General. Specifically, section 522(d)(3) requires the Inspector General to contract with an independent, third party that is a recognized leader in privacy and consulting, privacy technology, data collection and data use management, and global privacy issues, to:

- Evaluate the agency's use of information in an identifiable form;
- Evaluate the privacy and data protection procedures of the agency; and
- Recommend strategies and specific steps to improve privacy and data protection management.

The audit objectives, as required by Section 522, are to (1) evaluate the agency's use of information in identifiable form; (2) evaluate the privacy and data protection procedures of the agency; and (3) recommend strategies and specific steps to improve privacy and data protection management.

3. The FDIC's Wireless Communications

The FDIC provides laptop and personal data assistant users with the ability to send and receive corporate data and browse the Internet using wireless technology. While wireless technology provides greater access to corporate data and systems and improved process efficiencies, it also presents new security risks. Wireless networks are subject to the same risks as wired networks -- network intrusion, malicious code and viruses, unauthorized access, loss of data, compromise of data integrity, and data non-availability. Furthermore, because of the inherent portability and mobility provided by wireless technology, there is added risk of losing a wireless device.

The audit objective is to determine whether the FDIC has established and implemented security controls that provide reasonable assurance that its wireless communications are adequately protected.

4. Application Controls

The FDIC relies extensively on information systems to support its business operations. The FDIC's Division of Information Technology (DIT) maintains over 280 business applications in the Corporation's application inventory. The FDIC's business applications collect, process, store, and distribute sensitive information, such as personnel and bank data, in support of the Corporation's three primary program areas (Insurance, Supervision and Consumer Protection, and Receivership Management). The FDIC has classified 7 of its 284 business applications as major, which, according to OMB Circular A-130, Appendix III, requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, unauthorized access to, or modification of, the information in the application. It is essential that the FDIC's business application controls provide for the confidentiality, integrity, and availability of data.

The audit objective is to determine whether the FDIC has established and implemented controls to provide reasonable assurance of the confidentiality, integrity, and availability of data in its business applications.

5. The FDIC's IT Security Self-Assessment Program

Adequate security of information and the systems that process it is a fundamental management responsibility. Performing self-assessments provides a method for agency officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. In May 2005, GAO reported that the FDIC had not fully implemented an IT security self-assessment program to continually monitor its IT controls for potential weaknesses. Weaknesses in DIT's self-assessment practices could allow security weaknesses to go undetected, resulting in the compromise of systems and data. Any security breach could result in IT service interruptions or public embarrassment to the FDIC. DIT hired a contractor to develop and implement a security self-assessment program at the FDIC, and a senior FDIC official requested that the OIG conduct this audit.

The audit objective is to determine whether the FDIC's IT security self-assessment processes and practices are consistent with federal standards, guidelines, and recognized practices.

6. Information Enterprise Architecture

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

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

7. Integration of System Development and IT Capital Investment Processes

The FDIC is investing over \$100 million on six capital projects to develop and enhance a number of information systems to meet current and future business needs in resource management (budget, cost, and personnel); asset servicing and management; and performance of supervision and insurance functions. The FDIC has established and implemented controls over capital investment projects for developing or enhancing information systems. Specifically, the Capital Investment Review Committee provides the oversight by assessing the business case for the project, technical compliance with the FDIC's IT standards, and compliance against the FDIC's EA. The FDIC also recently

adopted the Rational Unified Process (RUP)[®] to improve the quality and timeliness of system development. One of the central best practices of the RUP[®] is the notion of developing systems iteratively. It is essential that the system development and the capital investment processes are well defined and coordinated to ensure that the cost, schedule, performance, and user expectation targets are met.

The audit objective is to 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.

Business Continuity Planning

1. Emergency Operations Plan

Recent large-scale disasters in the United States have clearly demonstrated how important it is to have reliable emergency response procedures and a well-written business continuity plan (BCP) to sustain critical business functions during an emergency or situation that may disrupt normal operations. The FDIC has developed an Emergency Operations Plan comprised of an ERP and a separate BCP. It is important, both symbolically and functionally, for federal government agencies to continue to serve the American public during any emergency or situation that may disrupt normal operations. An August 2004 OIG report on the *FDIC's Business Continuity Plan* found that the FDIC could improve the quality of its BCP in a number of key areas to help ensure its success should the BCP be implemented. Given our findings and the importance of this area, we believe a follow-up evaluation is warranted. The follow-up evaluation will include the FDIC's Emergency Operations Plan, which includes the ERP and BCP.

The objective is to evaluate the extent of the FDIC's progress in developing and implementing a comprehensive Emergency Operations Plan and implementing prior OIG recommendations.

2. IT Disaster Recovery Capability

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

recovery capability to Richmond, Virginia. Our audit will evaluate the FDIC's IT disaster recovery capability following the planned move to Richmond.

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

Enterprise Risk Management

1. Corporate Internal Control Program

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

The evaluation objective is to determine the extent to which the FDIC has implemented its internal control program consistent with applicable government-wide guidance and best practices.

Other Planned Assignment

In addition to audits, evaluations, and other reviews, the Office of Audits expends resources on other important matters as warranted. The following write-up reflects other planned work.

1. Peer Review of Another PCIE OIG's Audit Operations

OIGs are required by law to follow the Government Auditing Standards (GAS), issued by the Comptroller General. Audit organizations adhering to GAS are required to undergo an external peer review every 3 years. The FDIC OIG's Office of Audits participates in an external peer review program with members of the President's Council on Integrity and Efficiency.

The review objective is to determine whether the reviewed audit organization's internal quality control system is adequate to provide reasonable assurance that applicable auditing standards, policies, and procedures were met in conducting audits.

APPENDIX I: Ongoing Assignments

Insured Depositors Are Protected From Loss Without Recourse to Taxpayer Funding

Consideration of Examination Results in the Risk-Related Premium System

The audit objective is to determine whether the system used by the Division of Insurance and Research for charging deposit insurance premiums is adequately tied to the risks identified in the bank's recent Report of Examination by the primary federal regulator and other information the primary federal regulator and the FDIC determine to be relevant to the institution's financial condition and the risk posed to the deposit insurance funds.

FDIC-Supervised Institutions Are Safe and Sound

None

Consumers' Rights Are Protected and FDIC-Supervised Institutions Invest in Their Communities

The FDIC's Efforts to Address Predatory Lending

The audit objective is to determine the challenges faced and the efforts taken by the FDIC to identify, assess, and address the risks posed to institutions and consumers from predatory lending practices.

Bank Service Providers' Protection of Sensitive Customer Information

The audit objective is to assess the FDIC's examination coverage of bank service providers' protection of sensitive customer information.

Privacy of Sensitive Customer Information

The audit objective is to 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.

Recovery to Creditors of Receiverships is Achieved

DRR's Efforts to Recover Unclaimed Deposits

The audit objective is to determine whether the FDIC has adequate systems in place to accurately track and obtain the recovery of unclaimed deposits.

DRR's Protection of Personal Information Collected During Closings

The audit objective is to determine whether DRR adequately protects personal information collected and maintained for resolution and receivership functions.

Strategic Resources Are Effectively Managed

Assessments Process and Calculation of the Reserve Ratio

The audit objective is to determine whether the Division of Finance (1) has the proper controls in place to ensure that the FDIC accurately calculates, collects, and processes assessments of financial institutions; and (2) properly determines the designated reserve ratio.

Facilities Management

The audit objective is to determine whether the FDIC is adequately ensuring the economical and efficient management of the FDIC's Washington, D.C., facilities.

Contractor Billing Reviews

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

Use of Performance Measures

The evaluation objectives are to (1) evaluate the FDIC's progress in using the Government Performance and Results Act (GPRA) to manage performance and in communicating information to assist with congressional decision-making; (2) determine whether FDIC managers use GPRA information to manage their programs; and (3) determine whether FDIC employs any tools similar to the OMB Program Assessment Rating Tool to gauge program success.

EEO Discrimination Complaints Process

The objective is to evaluate the FDIC's discrimination complaint resolution process and management of the FDIC's formal complaints caseload.

The FDIC's Certification and Accreditation Program

The audit objective is to assess the FDIC's certification and accreditation policies, procedures, and practices for consistency with federal standards and guidance.

Asset Servicing Technology Enhancement Project

The audit objective is to determine whether the FDIC has established a control framework for ensuring the delivery of a quality system that meets corporate requirements and user needs in a timely and cost-effective manner.

Internal Employee Data Security

The audit objective is to evaluate the FDIC's policies, procedures, and practices for safeguarding personal employee information in hardcopy and electronic form.

Other

Assistance on the Audits of the FDIC's 2005 Financial Statements

The annual audits of the FDIC's financial statements require extensive use of database analysis, cyclical retrievals, statistical sampling, and data integrity testing. For the audits of the FDIC's calendar year 2005 financial statements, the OIG is assisting the GAO by providing data collection support in the following financial statement areas: operating expenses and allocations, anticipated failures, receivables, loan loss reserves, sensitive payments, contingent liabilities for anticipated failures, account reconciliations, and database security analyses.

Appendix II: Assignments by Directorate

Insurance, Supervision, and Receivership Management Audits

Michael Lombardi, Director, (202) 416-2431

Bruce Gimbel, Associate Director, (202) 416-2587

1. Assessment of Large Bank Risks (Page 5)
2. Material Loss Reviews (Page 7)
3. Use of FinCEN Data and Tools (Page 7)
4. Examination Assessment of FDIC-Supervised Institutions' Security of Consumer Data (Page 8)
5. Examination Assessment of Offshore Outsourcing of Data Services (Page 8)
6. Examination Coverage of Foreign Transactions (Page 9)
7. Examination Assessment of Interest Rate Risk (Page 9)
8. Examination Assessment of Electronic Banking (Page 10)
9. Examination Assessment of the Reliability of Appraisals (Page 10)
10. Examiner Use of HMDA Data to Identify Potential Discrimination (Page 11)
11. Community Reinvestment Act Examination Process (Page 11)
12. Supervisory Actions Taken for Compliance Violations (Page 12)
13. Impact of Credit Scoring Systems on Fair Lending Examinations (Page 12)
14. Planning for Large or Multiple Institution Failures (Page 13)

Systems Management and Security Audits

Mark Mulholland, Director, (202) 416-2944

Ben Hsiao, Associate Director, (202) 416-2117

1. The FDIC's Information Security Program--2006 (Page 18)
2. The FDIC's Compliance With Section 522 of the Consolidated Appropriations Act of 2005 (Page 18)
3. The FDIC's Wireless Communications (Page 19)

4. Application Controls (Page 19)
5. The FDIC's IT Security Self-Assessment Program (Page 20)
6. Information Enterprise Architecture (Page 20)
7. Integration of System Development and IT Capital Investment Processes (Page 20)
8. IT Disaster Recovery Capability (Page 21)

Corporate Evaluations and Audits

Marshall Gentry, Director, (202) 416-2919

Marilyn Kraus, Associate Director, (202) 416-2426

1. Deposit Insurance Application Process (Page 6)
2. Performance-based Contracting (Page 14)
3. Contract Administration (Page 15)
4. Classifying Salary Costs in the NFE (Page 15)
5. Information Technology Application Services Task Order Awards (Page 15)
6. Interagency Agreement with GSA Under the FEDSIM Contract (Page 16)
7. Contract File Management (Page 16)
8. Contractor Reviews and Audits (Page 17)
9. Succession Planning Efforts (Page 17)
10. Emergency Operations Plan (Page 21)
11. Corporate Internal Control Program (Page 22)

Appendix III: Assignments by Strategic Areas of Focus

Ensuring Safety and Soundness Through Effective Examinations, Enforcement and Follow-up

1. Material Loss Reviews (Page 7)
2. Examination Assessment of Interest Rate Risk (Page 9)
3. Examination Assessment of Electronic Banking (Page 10)
4. Examination Assessment of the Reliability of Appraisals (Page 10)

Contributing to Public Confidence in Insured Institutions

5. Use of FinCEN Data and Tools (Page 7)
6. Examination Assessment of FDIC-Supervised Institutions' Security of Customer Data (Page 8)
7. Examination Assessment of Offshore Outsourcing of Data Services (Page 8)
8. Examination Coverage of Foreign Transactions (Page 9)

Managing Risks to the Insurance Funds

9. Assessment of Large Bank Risks (Page 5)
10. Deposit Insurance Application Process (Page 6)

Ensuring Compliance with Consumer Protection and Fair Lending Laws

11. Examiner Use of HMDA Data to Identify Potential Discrimination (Page 11)
12. Community Reinvestment Act Examination Process (Page 11)
13. Supervisory Actions Taken for Compliance Violations (Page 12)
14. Impact of Credit Scoring Systems on Fair Lending Examinations (Page 12)

Being Ready for Potential Institution Failures

15. Planning for Large or Multiple Institution Failures (Page 13)

Managing and Securing Financial, Human, IT, and Procurement Resources

16. Performance-based Contracting (Page 14)
17. Contract Administration (Page 15)
18. Classifying Salary Costs in the NFE (Page 15)
19. Information Technology Application Services Task Order Awards (Page 15)
20. Interagency Agreement with GSA Under the FEDSIM Contract (Page 16)
21. Contract File Management (Page 16)
22. Contractor Reviews and Audits (Page 17)
23. Succession Planning Efforts (Page 17)
24. The FDIC's Information Security Program--2006 (Page 18)
25. The FDIC's Compliance With Section 522 of the Consolidated Appropriations Act of 2005 (Page 18)
26. The FDIC's Wireless Communications (Page 19)
27. Application Controls (Page 19)
28. The FDIC's IT Security Self-Assessment Program (Page 20)
29. Information Enterprise Architecture (Page 20)
30. Integration of System Development and IT Capital Investment Processes (Page 20)
31. Emergency Operations Plan (Page 21)
32. IT Disaster Recovery Capability (Page 21)
33. Corporate Internal Control Program (Page 22)