Office of Inspector General

September 2006
Report No. 06-022

Independent Evaluation of the FDIC's Information Security Program-2006

AUDIT REPORT

Office of Audits

OIG

Office of Audits

OIG

Background and Purpose of Evaluation

The FDIC's mission is to contribute to the stability and public confidence in the nation's financial system by insuring deposits, examining and supervising financial institutions, and managing receiverships. To achieve its mission, the FDIC relies on automated information systems to collect, process, and store vast amounts of banking and other sensitive information. Much of this information is used by financial regulators, academia, and the public to monitor bank performance, develop regulatory policy, and conduct research on and analysis of important banking issues. Ensuring the integrity, availability, and appropriate confidentiality of this information in an environment of increasingly sophisticated security threats and global connectivity requires a strong, enterprise-wide information security program.

The objective of the evaluation was to determine the effectiveness of the FDIC's information security program and practices, including the FDIC's compliance with the Federal Information Security Management Act of 2002 (FISMA) and related information security policies, procedures, standards, and guidelines.

To view the full report, go to www.fdicig.gov/2006reports.asp

Report No. 06-022
September 2006

Independent Evaluation of the FDIC's Information Security Program-2006

Results of Evaluation

As a result of focused efforts over the last several years, the FDIC has made significant progress in improving its information security program and practices. Further, additional improvements were underway at the time of our evaluation. Our work did not identify any significant deficiencies in the FDIC's information security program that warrant consideration as a potential material weakness as defined by the Office of Management and Budget. However, as shown in the table below, continued management attention is needed in key security control areas to ensure that appropriate risk-based and cost-effective security controls are in place to secure the FDIC's information resources in furtherance of the Corporation's security program goals and objectives. Therefore, we concluded that the FDIC had established and implemented internal controls that provided limited assurance of adequate security for its information resources. Our report includes a number of steps that the Corporation can take to strengthen its information security program and practices.

Office of Inspector General (OIG) Assessment of the FDIC's Security Program Controls

Control Class	Control Families Tested That Demonstrate Effectiveness	Control Families Tested That Warrant Management Attention
Program	• Information Security Governance	• Enterprise Architecture • Capital Planning
Management	• Risk Assessment • Planning	• Certification, Accreditation, and Security Assessments
Operational	• Contingency Planning • Incident Response • Awareness and Training	• Personnel Security • Physical Security and Environmental Protection • Configuration Management • Maintenance • System and Information Integrity • Media Protection
Technical	• Identification and Authentication	• Access Control • Audit and Accountability

Source: 2006 FDIC OIG Evaluation of the FDIC's Information Security Program.

TABLE OF CONTENTS

TABLES

FIGURES

FDIC Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226 Office of Inspector General

DATE: September 27, 2006

MEMORANDUM TO: Sheila C. Bair, Chairman
Federal Deposit Insurance Corporation

FROM: Jon T. Rymer
Inspector General

SUBJECT: *Independent Evaluation of the FDIC's Information Security Program-2006*
(Report No. 06-022)

As required by the Federal Information Security Management Act of 2002 (FISMA), we have completed an independent evaluation of the FDIC's information security program and practices. FISMA directs federal agencies to have an annual independent evaluation performed of their information security program 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 (IG) or an independent external auditor as determined by the IG. We issued separate audit reports to the Chief Information Officer (CIO) and Chief Privacy Officer that contain responses to specific sections of the July 17, 2006 OMB memorandum entitled, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.[1] Our responses to the OMB questions, together with this independent security evaluation report, satisfy our 2006 FISMA reporting requirements. In addition, we plan to issue a separate report to the CIO that contains more detailed information about the security control deficiencies discussed in this report and make appropriate recommendations, if necessary, at that time.

The objective of our evaluation was to determine 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. Details regarding the evaluation's scope and methodology are presented in Appendixes I and II, and an acronyms list is provided in Appendix III. A glossary of terms used in this report is provided in Appendix IV.

As our report details, the FDIC has made significant progress in addressing current and emerging security standards and guidelines developed by the National Institute of Standards and Technology (NIST). However, continued management attention is

[1] *Responses to Security-Related Questions in OMB's Fiscal Year 2006 Reporting Instructions for FISMA and Agency Privacy Management*, dated September 22, 2006 (Report No. 06-019) and *Response to Privacy Program Information Request in OMB's Fiscal Year 2006 Reporting Instructions for FISMA and Agency Privacy Management*, dated September 22, 2006 (Report No. 06-018).

warranted in key security control areas to ensure that appropriate risk-based and cost-effective security controls are implemented to secure the FDIC's information resources. Our work did not identify any significant deficiencies in the FDIC's information security program that warrant consideration as a potential material weakness as defined by the OMB.[2]

Similar to our prior-year security evaluations, we identified key steps (listed in priority order below) that the Corporation can take to improve the effectiveness of its information security program controls. These steps are targeted to address the control areas in which the opportunity to improve performance is the greatest. In many cases, the FDIC was already working to address these steps during our evaluation field work.

(1) Continue to place priority attention on certifying and accrediting the FDIC's non-major application systems that process sensitive data.

(2) Develop a risk-based, enterprise-wide approach for (a) monitoring user access privileges in information systems and (b) generating and reviewing audit logs for the FDIC's inventory of information systems.

(3) Ensure that all sensitive data stored on mobile FDIC computing devices is encrypted consistent with OMB's June 23, 2006 memorandum entitled, *Protection of Sensitive Agency Information*.

(4) Complete the FDIC's information security risk management program methodology by defining procedures for performing (a) continuous monitoring of system security controls after accreditation and (b) contingency planning for systems.

(5) Define more fully the FDIC's information security standards and integrate these standards into the Corporation's enterprise architecture (EA).[3]

(6) Enhance the FDIC's inventory of information systems by: (a) identifying systems used or operated by contractors and other organizations on behalf of the FDIC; (b) including interfaces between each system in the inventory and all other systems and networks, including those not operated by or under the control of the FDIC; and

---

[2] The OMB defines a significant deficiency as a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified, and immediate or near-immediate corrective action must be taken. The OMB defines a material weakness as a significant deficiency that the agency head determines to be significant enough to be reported outside the agency (i.e., included in the annual management control report to the President and the Congress).

[3] An EA is an agency-wide blueprint that defines, in both business and technological terms, an organization's current and target operating environments and the organization's transition between the two. Among other things, the EA defines principles and goals for, and sets direction on, information technology (IT) security. Although the FDIC is not legally required to develop an EA, the FDIC recognizes the value of having an EA and is working to implement an EA.

(c) leveraging the EA to centrally manage, track, and report risk-management related information, such as system categorization and test and authorization dates.

(7) Strengthen oversight of contractors with access to sensitive information and systems by (a) ensuring that contractor IT equipment connected to the FDIC's network are routinely scanned for security vulnerabilities and the results are addressed in a timely manner and (b) ensuring that confidentiality agreements are executed in accordance with FDIC policy.

(8) Strengthen change-control procedures related to mainframe system software to ensure that system software programs are formally documented and that changes are formally controlled and approved.

(9) Improve the FDIC's information security cost management practices in order to facilitate resource and investment decisions.

As part of its audit of the FDIC's calendar year 2005 financial statements,[4] the Government Accountability Office (GAO) identified a number of information security control weaknesses in the FDIC's information systems controls that are designed to protect the confidentiality, integrity, and availability of key financial information and information systems. The collective severity of these weaknesses were such that GAO considered them to be a reportable condition[5] as of December 31, 2005 because the weaknesses increased the risk of unauthorized modification and disclosure of critical FDIC financial and sensitive personnel information, disruption of critical operations, and loss of assets.

In its response to GAO's conclusions, the FDIC acknowledged but did not share the GAO's assessment of the severity of the risk impact or magnitude of the collective vulnerability posed by the control issues identified by GAO. However, the FDIC indicated that it would work with GAO to reconcile both organizations' respective views and augment its information security program and practices in those instances where FDIC and GAO determine that changes are appropriate. In August 2006, GAO issued a report to the FDIC's Board of Directors related to the 2005 Financial Statements.[6] GAO recommended that the FDIC Chairman fully implement key elements of its agency-wide information security program. We will consider the FDIC's actions in response to GAO's recommendations as part of our next annual FISMA evaluation.

In view of the collective risk associated with the results of our independent security program assessment and GAO's financial statement audit, the FDIC should consider

---

[4] *FINANCIAL AUDIT Federal Deposit Insurance Corporation Funds 2005 and 2004 Financial Statements*, dated March 2006 (Report No. GAO-06-146).

[5] The reportable condition in information system controls, although not considered material, represents a significant deficiency in the design or operation of internal control that could adversely affect the FDIC's ability to meet its internal control objectives.

[6] *INFORMATION SECURITY Federal Deposit Insurance Corporation Needs to Improve Its Program*, dated August 2006 (Report No. GAO-06-620).

including the information security program as an area of high priority for management attention in the annual statement of assurance on internal accounting and administrative control required by the Chief Financial Officers Act and Federal Managers Financial Integrity Act (FMFIA). Such treatment will help ensure appropriate senior management visibility in order to address information security program risks. Appendix I contains additional information about information-security-related laws, regulations, and other guidance.

The FDIC's Office of Inspector General (OIG) will continue to work with the Corporation throughout the coming year to ensure that appropriate risk-based and cost-effective information security controls are in place to secure the Corporation's information resources and achieve its security goals and objectives.

BACKGROUND

Title III of the E-Government Act of 2002, commonly referred to as FISMA, focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA requires federal agencies to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The Act assigns specific responsibilities to agency heads, IGs, OMB, and NIST. The FDIC has determined that aspects of FISMA apply to the Corporation.

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of FISMA and related policies, procedures, standards, and guidelines. FISMA directs federal agencies to report annually to the OMB Director, Comptroller General, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with FISMA. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG. OMB has responsibility for overseeing agency information security policies and practices and reporting annually to the Congress on agency compliance with FISMA requirements. OMB's primary agency security policy is OMB Circular No. A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources* (OMB A-130, Appendix III), dated November 28, 2000.[7]

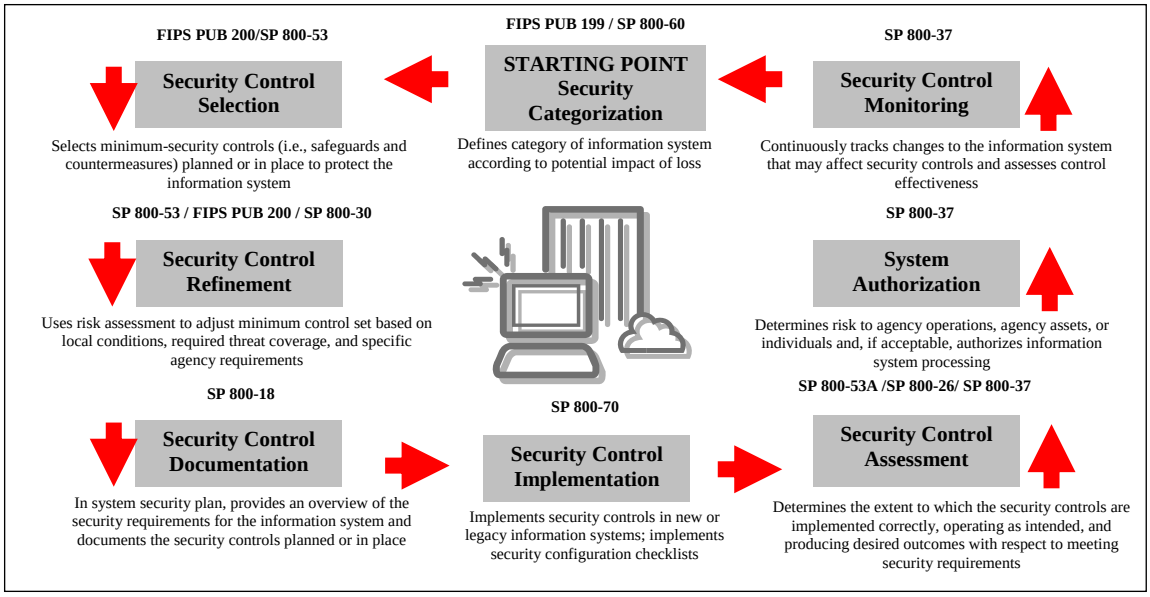
FISMA directs NIST to develop risk-based standards and guidelines to assist agencies in defining minimum security requirements for the non-national security systems used by agencies.[8] NIST has developed such standards and guidelines as part of its FISMA Implementation Project and is developing additional standards and guidelines. NIST standards and guidelines are introducing significant changes in the manner in which federal agencies, including the FDIC, protect their information and information systems. Figure 1, on the following page, illustrates the relationship of key NIST security standards and guidelines. Of those NIST security standards and guidelines shown in the

[7] OMB A-130, Appendix III was last revised on February 8, 1996 and was republished on November 28, 2000. Various provisions of that appendix are legally binding on the FDIC.

[8] FISMA authorizes the Secretary of Commerce to make NIST standards compulsory for executive agencies to the extent determined necessary to improve the efficiency and security of federal information systems. The Secretary of Commerce exercises this authority subject to the direction of the President and in coordination with the OMB Director. Whether a NIST publication is legally binding upon the FDIC depends on the nature of the publication and the statutory basis(es) under which the publication was promulgated.

figure, NIST finalized Federal Information Processing Standards Publication (FIPS PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*, and published drafts of Special Publication (SP) 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*; and SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, following our 2005 evaluation.[9] Security program officials should consider whether it is prudent for their agencies to implement draft NIST standards and guidelines (or portions thereof) before the standards and guidelines become effective.

Figure 1: Managing Enterprise Risk (The Framework)



Source: NIST.

Corporate policies and procedures related to the internal operation of the FDIC that affect more than one FDIC division or office are published through the FDIC Directives System. In addition to using other corporate-wide policies and procedures, the FDIC uses the Directives System to issue information security policy, procedure, and guidance of FDIC-wide interest. The FDIC's Division of Administration (DOA) administers the FDIC Directives Management Program, including the review of proposed directives for conformance to editorial standards, distribution of final directives, documentation of the change process for directives, and maintenance of current and historical versions of the corporate directives. The FDIC's Division of Information Technology (DIT) has established and administers additional internal policies and procedures related to DIT operations.

[9] NIST issues information security standards as FIPS PUBs and information security guidance as Special Publications (SP). Appendix I provides additional information about FIPS PUBs and SPs, including the applicability of these publications to the FDIC.

FDIC Systems and Applications

The FDIC relies extensively on information systems to support its business operations. DIT maintains 8 general support systems[10] that provide basic processing and communications support for the 279 business application systems[11] in the Corporation's application inventory. The FDIC's business applications collect, process, store, and distribute mission-critical 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 seven of the business application systems as major applications.[12] Table 1 identifies the FDIC's general support systems and major applications.

Table 1: The FDIC's General Support Systems and Major Applications

General Support Systems	Mainframe
	Remote Access
	Voice/Video
	Mid-range Servers
	Local Area Network/Wide Area Network (LAN/WAN)
	Windows 2000 Servers
	Public Key Infrastructure
	Personal Systems
Major Applications	New Financial Environment
	Legal Integrated Management System
	Assessment Information Management System II
	Risk-Related Premium System
	Virtual Supervisory Information on the Net
	Receivership Liability System
	FDIC*connect*

Source: DIT risk management inventory as of August 29, 2006.

[10] OMB A-130, Appendix III, defines a general support system as an interconnected set of information resources under the same direct management and that shares common functionality. A system normally includes hardware, software, information, applications, communications, and people.

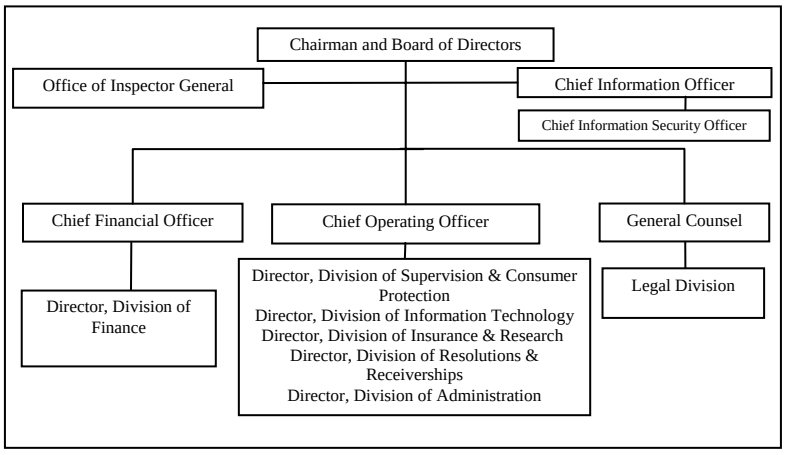
[11] According to the *Application Systems Baseline Inventory* management report as of July 31, 2006. The August 29, 2006 DIT Information Security Staff (ISS) risk management inventory, used for FISMA reporting, identified 165 FDIC information systems—150 systems from the *Applications Systems Baseline Inventory*, 8 general support systems, and 7 contractor systems not included in the *Application Systems Baseline Inventory*. According to ISS, the remaining 129 systems of the *Application Systems Baseline Inventory* were no longer in service, or were tools, utilities, configurations, or other objects that were not application systems and, therefore, were not included in the ISS risk management inventory.

[12] OMB A-130, Appendix III, defines a major application as one that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application.

Information Technology Security Governance

Several key components comprise the FDIC's IT security governance structure. As illustrated in Figure 2, these components include the FDIC Chairman and Board of Directors; CIO; Chief Operating Officer (COO); Chief Financial Officer (CFO); and the Directors of DIT, DOA, and other divisions and offices that own information systems. The Chairman and Board of Directors are ultimately responsible for the security of the FDIC's information and information systems. The CFO and CIO co-chair a Capital Investment Review Committee (CIRC), which reviews and monitors capital projects, including IT projects. The CIO has responsibility for the FDIC's information security program, including FISMA compliance. The CIO also serves as the FDIC's Chief Privacy Officer and Director, DIT. In addition, a CIO Council, composed of senior agency managers, advises the CIO on all aspects of IT, including security. The COO manages the FDIC's operating divisions, including DIT and DOA. DIT is responsible for providing a secure IT infrastructure and systems. DOA is responsible for providing physical and personnel security for the FDIC. Other division and office heads are responsible for ensuring that systems under their ownership or control conform to the FDIC's security requirements. The OIG performs audits and evaluations of the FDIC's information security controls, including the annual independent evaluation of the Corporation's security program required by FISMA.

Figure 2: The FDIC's IT Security Governance



Source: OIG Analysis of FDIC's roles and responsibilities.

The CIO has assigned primary responsibility for planning, developing, and implementing the FDIC's information security program and operations to an Associate Director in DIT, who reports directly to the CIO. In addition, the FDIC has established eight Information Security Managers (ISMs) within its program divisions and offices to ensure a business focus on information security. The responsibilities of ISMs include promoting security awareness, providing security management and technical advice on behalf of their divisions and offices, and assessing the level of security needed and in place in FDIC's system's and applications. DIT's operating and capital investment budget for calendar year 2006 is approximately $191 million, of which approximately $16 million related to IT security.

DOA's Security Management Section is responsible for administering the FDIC's physical and personnel security programs. Physical security includes activities such as

badging employees, contractors, and visitors and protecting employees, visitors, and facilities from internal and external threats such as fire, theft, vandalism, sabotage, and terrorist activities. Personnel security includes activities such as performing credit checks, fingerprint checks, and background investigations of FDIC employees and contractors. The Security Management Section is also responsible for managing, directing, and testing the FDIC's Emergency Preparedness Program, which includes the FDIC's Emergency Response Plan and the Business Continuity Plan (BCP). DIT and DOA coordinate on relevant corporate security matters.

Environmental factors also impacted information security at the FDIC during the past year. For example, following our 2005 security evaluation, the FDIC vacated 3 leased office buildings in Washington, D.C., and moved about 750 employees and contractors to a newly completed expansion of its Arlington, Virginia, facility. In addition, the FDIC has established a new disaster recovery data center to provide the Corporation with a more robust disaster recovery architecture and full control over its disaster recovery capability. These areas presented additional challenges in physical security for the FDIC's information security.

According to the June 2006 DIT Monthly Status Report, DIT completed a pilot project, in June 2006, to apply the principles of the Control Objectives for Information and related Technology (COBIT®)[13] to the FDIC's IT processes. As part of the project, DIT developed a new, automated risk assessment and process maturity tool that focuses on IT-specific processes and control objectives. DIT completed an initial mapping of its organization and functions to the COBIT® framework and is now updating management control plans to reflect a process orientation to replace its former organizational and functional orientation. The COBIT® approach recognizes that many IT responsibilities are shared across the organization and must be treated in an enterprise-wide manner. Further, DIT is identifying process owners who will be charged with understanding and monitoring the internal controls over an entire process rather than those that fall within their organizational boundaries.

Prior-Year Security Control Evaluations

In previous years, based on our analysis of long-standing requirements in security-related statutes, policies, and guidance and consideration of the FDIC's business and IT environment, we identified key management control areas associated with the FDIC's information security program. For each of the management control areas, we provided an assessment in terms of the level of assurance that the management control provided adequate security over the FDIC's information resources. Using each of the management control assessments as a basis and considering associated risks, we evaluated the Corporation's overall information security program and compared it to previous security evaluation results. In this manner, we were able to evaluate the FDIC's progress in strengthening its information security program and practices.

[13] COBIT® is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues, and business risks. COBIT® enables clear policy development and good practice for IT control throughout organizations.

Federal security control requirements and assessment methodologies have changed dramatically in recent years in response to new NIST security standards and guidelines. As a result, we modified our prior-year security program assessment methodology to be consistent with the security control framework defined in FIPS PUB 200 for protecting the confidentiality, integrity, and availability of information and information systems. Additionally, NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, builds upon FIPS PUB 200 by defining a framework comprised of three general classes of security controls (i.e., management, operational, and technical) that collectively contain the 17 security control families identified in FIPS PUB 200.[14] We included one additional control class (i.e., program) in our assessment methodology based on our research of relevant security-related statutes, regulations, policies, and guidelines. Due to the magnitude of the changes in our assessment methodology, we determined that a direct comparison of our current year results to prior year results would not be performed this year. Appendixes I and II provide a detailed description of our new security program assessment methodology.

[14] Federal agencies must meet the minimum security requirements defined in FIPS PUB 200 through the use of the controls in SP 800-53. The applicability of these publications to the FDIC has not been determined.

RESULTS OF EVALUATION

The FDIC has made significant progress in recent years in addressing the information security requirements of FISMA and NIST, and additional security control improvements were underway at the time of our evaluation. This progress is noteworthy given the considerable increase in security-related requirements. In particular, the FDIC has certified and accredited all but one of its major applications[15] and general support systems consistent with NIST security standards and guidelines. Additionally, the FDIC had revised its information security-risk management methodology in June 2006 to achieve cost-efficiencies in its certification and accreditation program. Further, the FDIC has established a new organizational structure as part of its IT program transformation, consolidated many of its IT security-related contracts, and implemented a new corporate IT disaster recovery capability. These accomplishments are notable; however, continued management attention is warranted in a number of key security control areas to ensure that appropriate risk-based and cost-effective security controls are in place.

We structured the results of our security program assessment according to the security control framework defined in FIPS PUB 200 and SP 800-53. We included one additional control class (i.e., program) in our results based on our research of relevant security-related statutes, regulations, policies, and guidelines.

Based on our security program assessment, we concluded that the FDIC's program, management, operational, and technical security controls collectively provided limited assurance of adequate security over corporate information resources. However, our work did not identify any significant deficiencies in the FDIC's information security program that warrant consideration as a potential material weakness as defined by the OMB.[16] Table 2, on the following page, summarizes our assessment results based on the security control testing we performed.[17]

[15] The CIO provided the FDIC's New Financial Environment system with an interim authorization to operate while the FDIC addresses security risks identified during the certification and accreditation process. Information systems are not certified and accredited during the interim authorization period.

[16] FISMA requires agencies to report any significant deficiency in a policy, procedure, or practice as a material weakness in reporting under the FMFIA. FMFIA requires agencies to evaluate their internal control systems on an annual basis and to report the results of the evaluation, along with any material weaknesses and plans for corrective actions, to the President and the Congress. These requirements were made applicable to the FDIC by the Chief Financial Officers Act of 1990.

[17] Our evaluation did not include an assessment of the *System and Communications Protection* or the *Systems and Services Acquisition* control families. Appendix II describes the security control testing we performed within each control family.

Table 2: OIG Assessment of the FDIC's Security Controls

Control Class	Control Families Tested That Demonstrate Effectiveness	Control Families Tested That Warrant Management Attention
Program	• Information Security Governance	• Enterprise Architecture • Capital Planning
Management	• Risk Assessment • Planning	• Certification, Accreditation, and Security Assessments
Operational	• Contingency Planning • Incident Response • Awareness and Training	• Personnel Security • Physical Security and Environmental Protection • Configuration Management • Maintenance • System and Information Integrity • Media Protection
Technical	• Identification and Authentication	• Access Control • Audit and Accountability

Source: 2006 OIG Evaluation of the FDIC's Information Security Program.

PROGRAM CONTROLS

Program controls define an enterprise-wide framework for planning, directing, and controlling resources to achieve agency security objectives. Based on our analysis of relevant security-related statutes, regulations, policies, standards, and guidelines, we identified three program control families to include in our FISMA evaluation this year: *Information Security Governance*, *Enterprise Architecture*, and *Capital Planning*. In summary, the controls we tested in the area of *Information Security Governance* were effective. However, the controls we tested related to *Enterprise Architecture* and *Capital Planning* warranted management attention.

Information Security Governance

Information security governance involves the implementation of an enterprise-wide control structure that provides management with reasonable assurance that its security goals and objectives are being achieved. Governance consists of enterprise-wide security program policies and procedures that define key roles and responsibilities and monitoring to assess whether security controls are achieving intended results. FISMA defines specific responsibilities and authorities for agency heads,[18] senior agency officials, and CIOs. Among those responsibilities are requirements for the CIO to develop and maintain an information security program and report annually to the agency head on the effectiveness of the program and progress of remedial actions.

The FDIC has appointed a permanent CIO with corporate accountability and authority for information security, a senior agency information security officer who reports directly to the CIO, and a CIO Council composed of senior agency managers who advise the CIO on all aspects of IT. The FDIC has established a number of policies, procedures, and guidelines that generally define the security roles and responsibilities of corporate officials and contractor personnel. In addition, DIT published a new *Information Security Strategic Plan,* and the CIO made periodic presentations to senior agency officials, including the FDIC Audit Committee, on corporate information security initiatives and efforts to remediate information security weaknesses.

Following our 2005 security evaluation, DIT also began implementing a COBIT®-based internal control review program and included six security-related metrics in its divisional performance reports. Such control improvements are important for ensuring that corporate security goals and objectives are attained. To further enhance its information security governance, the FDIC should consider additional measures. Specifically, the FDIC can promote greater corporate awareness of security roles and responsibilities by formally coordinating through DOA on security-related policies, procedures, and memoranda issued by divisions, offices, and corporate committees. We noted that some

[18] For the purposes of our evaluation, we consider the FDIC's Chairman to be the head of the Corporation. Nevertheless, the FDIC's Board of Directors, by statute, has overall responsibility for managing the Corporation. The Board consists of five members: the Chairman, Vice Chairman, Director, Director of the Office of Thrift Supervision, and Comptroller of the Currency.

internal DIT security policies and procedures posted on its internal Web site defined security roles and responsibilities of personnel in other FDIC divisions and offices.

While the FDIC has components of a sound information security governance structure in place, such as the CIRC and CIO Council, the Corporation could also benefit from clearly articulating overall information security governance roles, responsibilities, and relationships, including those of senior agency management. Draft SP 800-100, dated June 2006, entitled, *Information Security Handbook: A Guide for Managers,* suggests that agencies should integrate their information security governance activities with the overall agency structure and activities by ensuring appropriate participation of agency officials in overseeing implementation of information security controls throughout the agency. Further, new and evolving security requirements and recent highly publicized data security breaches involving federal agencies underscore the importance of senior management oversight of security. Industry research also suggests that a powerful approach to achieving effective integration of enterprise security risk management is implementing a business-focused "council" of senior organization leaders to provide governance of security program activities.

Enterprise Architecture

An EA defines, in business and technological terms, an organization's current and target operating environments, including its IT security architecture. Effectively representing security information in an EA ensures that security is adequately incorporated into agency system life-cycle processes, as required by FISMA. In addition, FISMA requires agencies to develop and maintain an inventory of major information systems, which is a fundamental component of an agency EA.

The FDIC has taken a number of important steps toward full implementation of a corporate-wide EA. Of particular note, the FDIC has established an EA policy and EA governance structure, adopted a system development life-cycle (SDLC) methodology,[19] and developed an EA repository to store, classify, and organize its EA data (including security data). Additionally, the FDIC hired a Deputy Director, Enterprise Technology Branch, in May 2006 and a Chief Enterprise Architect in July 2006 to further its EA program.

While these steps are positive, more work remains to fully define the FDIC's IT security architecture and use this information as part of an applied EA. DIT officials indicated that they were working to update two key EA components (the FDIC Technical Reference Model[20] and Security Standards Profile[21]) and integrate them into the EA repository. Once completed, DIT will need to define procedures for the development,

[19] The FDIC's Rational Unification Process (RUP®) SDLC methodology includes FDIC-specific security requirements applicable to each phase of the development of an IT project.

[20] The Technical Reference Model identifies and describes, among other things, the security services used throughout the agency.

[21] The Security Standards Profile identifies the security standards specific to the security services (such as access control and authentication) specified in the agency's EA.

maintenance, and use of its EA repository. Such procedures will provide assurance that information systems are consistent with an approved security architecture.[22] The FDIC should leverage its existing EA repository to centrally manage, track, and report risk-management-related information, such as security categorizations and test and authorization dates. Further, the FDIC needed to update its inventory of information systems to identify contractor systems and systems' interfaces with all other systems or networks, including those not operated by or under the control of FDIC, as required by FISMA. Once fully implemented, the EA repository is expected to provide an automated, comprehensive, accurate, and dynamic system inventory and baseline of the FDIC's approved IT security architecture.

On June 1, 2006, the Federal CIO Council published *The Federal Enterprise Architecture Security and Privacy Profile*, version 2.0. This profile can provide the FDIC with valuable guidance on incorporating security into the FDIC's EA.

Capital Planning

OMB Circular A-130 defines the capital planning and investment control process as the ongoing process for identifying, selecting, controlling, and evaluating IT investments.[23] The circular states that investments in new or existing information systems must demonstrate that the cost of security controls are understood and explicitly incorporated into the life-cycle planning of the overall system. The circular also states that the costs of system security controls must be commensurate with the risk and magnitude of harm that could result from the loss, misuse, unauthorized access to, or modification of the information stored or flowing through the system. In addition, the OMB has issued policy and guidance requiring agencies to (1) integrate security into the life cycle of their systems development, modernization, and enhancement efforts and (2) ensure steady-state operations meet existing security requirements before new funds are spent on systems development, modernization, or enhancements.[24] FISMA states that agency heads are responsible for ensuring that information security management processes are integrated with agency strategic and operational planning.

The FDIC established and implemented a number of key controls for integrating security into the life-cycle planning and management of its capital IT investments. Specifically, the FDIC has an *Information Technology Strategic Plan*, which includes a key goal related to information security, and published an *Information Security Strategic Plan* in 2006 to help ensure that security is integrated into the FDIC's strategic and operational planning. Also, the FDIC has developed a formal CPIM program to plan and manage its

[22] Recent GAO and OIG audits identified internal control weaknesses relating to security policies and standards that had not been adequately incorporated into the design of FDIC information systems.

[23] The FDIC is voluntarily implementing (i.e., is not required by statute) a capital planning and investment control process, referred to as the capital planning and investment management (CPIM) process.

[24] Such OMB policy and guidance includes, but is not limited to, Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, and Memoranda M-00-07, *Incorporating and Funding Security in Information Systems Investments*; and M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments.*

capital IT investments; established corporate committees[25] to evaluate whether information and physical security is adequately addressed in proposed capital IT investments; and established a series of accounting codes in its accounting system to identify and track certain security-related costs. These accomplishments are notable; however, more work is needed to ensure that security is fully integrated into the life-cycle management of the FDIC's IT investments.

At the time of our evaluation, the FDIC was working to define procedures in its RUP® systems development methodology and related guidance for project-level reporting and interaction with the FDIC Enterprise Architecture Board.[26] Such procedures will provide assurance that security controls being considered for capital investment projects are adequately evaluated for consistency with the FDIC's security architecture. Regarding security costs, the FDIC estimates and tracks certain security costs, such as the costs of performing security testing and evaluation (ST&E) (i.e., security assessments), associated with its capital IT investments[27] as part of its CPIM process. However, as we have reported in our prior-year security evaluation reports, the FDIC's budget formulation process differs from the processes followed by other agencies that are bound by the federal appropriations process. The FDIC devotes less attention to security program cost management than required at appropriated agencies. For example, the FDIC generally does not, and is not required to:

- Identify and track security program costs consistent with OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*; and SP 800-65, *Integrating IT Security Into the Capital Planning and Investment Control Process*.
- Estimate the resources required to remediate individual security weaknesses on Plans of Action and Milestones (POA&Ms) as described in OMB's FISMA reporting instructions.
- Allocate security program costs to its major IT investments.[28]

We plan to work with the Corporation in the coming year to explore measures that the FDIC can take to strengthen its security cost management practices. Such measures may

[25] The CIRC and the CIO Council have responsibilities for reviewing, recommending, and monitoring corporate IT investments.

[26] The Board is responsible for recommending cost-effective and efficient corporate solutions by evaluating the degree to which proposed projects align with the target EA.

[27] The FDIC generally defines capital investments as projects that have a total investment budget of $3 million or more and other projects deemed to have significant corporate impact. The FDIC prepares a business case containing an aggregate security cost estimate for each capital investment. However, the security cost estimates are used for informational purposes only and are not determined through an analysis of historical costs. At the close of our evaluation, the FDIC was managing three capital investment projects.

[28] NIST SP 800-65 defines a major IT investment as, among other things, a system or investment that requires special management attention because of its importance to an agency's mission or is an integral part of the agency's EA. The financial justification for one such project at the FDIC, the Deposit Insurance Reform project, did not identify how much of the $9.6 million cost estimate related to information security.

include, for example, the development of written guidance to ensure that IT security costs are consistently identified, tracked, and reported at both the IT project and corporate levels.

MANAGEMENT CONTROLS

Management controls are the safeguards or countermeasures related to an information system that focus on the management of risk and system security. SP 800-53 divides management controls into four control families: *Risk Assessment*; *Planning*; *System and Services Acquisition*; and *Certification, Accreditation, and Security Assessments*. In summary, we found that the controls we assessed in the areas of *Risk Assessment* and *Planning* are effective. However, the controls assessed in the area of *Certification, Accreditation, and Security Assessments* warrant management attention. Due to our limited testing of *System and Services Acquisition* controls, we did not assess this control family as part of our current-year work.

Risk Assessment

Risk is the probability of an adverse event occurring. Risk assessment involves the implementation of policies, procedures, and practices for categorizing information and systems, performing and updating system risk assessments, and performing regular system vulnerability scanning. Under FISMA, agencies are responsible for providing security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems.

The FDIC developed and implemented risk assessment policies and procedures for FDIC-owned and operated systems that were generally consistent with NIST security standards and guidelines. Regarding its LAN/WAN system, the FDIC was scanning LAN/WAN equipment for security vulnerabilities on a regular basis and taking appropriate remedial actions. In addition, our independent testing of a sample of LAN/WAN routers and switches found that their security configurations were generally consistent with defined security baseline configurations.

Following our 2005 security evaluation, DIT developed procedures for performing monthly vulnerability scans of contractor-owned computers connected to the FDIC's network. We noted that DIT performed monthly vulnerability scans of such contractor-owned computers through March 2006 but that the scans had not been performed in April or May 2006. In addition, some, but not all, contractor-owned computers connected to the network were scanned in June and July 2006. We spoke with DIT officials about this matter and learned that contractor-owned computers were not scanned during the referenced periods due to a technical error. The FDIC is heavily dependent on contractors to provide IT development and support activities and has recently sought to physically locate contractor staff in FDIC facilities to reduce costs and security risks. The FDIC can achieve greater security assurance by ensuring that all contractor-owned computers connected to the network are identified and scanned for vulnerabilities on a monthly basis as described in DIT's IT security self-assessment procedures.

Planning

Planning involves the implementation of policies, procedures, and practices for developing system security plans. Security plans provide an overview of system security requirements and describe the security controls in place or planned for meeting those requirements. Planning also involves establishing rules that describe user responsibilities and expected behavior related to system usage, as well as conducting system privacy impact assessments (PIA).[29]

The FDIC's security planning policies and procedures were generally consistent with NIST security standards and guidelines. However, guidance for preparing system security plans should be enhanced to require that security plans describe how common security controls[30] are considered in the security certification and accreditation (C&A) process described later in this report. ST&E of common security controls are performed separately from ST&E of application and general support system security controls. Therefore, enhancing guidance for preparing system security plans would provide greater assurance that all relevant risks are considered when accrediting an application or system and promote efficiency because common controls are assessed in separate ST&Es. Regarding PIAs, the FDIC has developed procedures for performing PIAs of its systems containing information in an identifiable form.[31] As reported in our Audit Report No. 06-018, the FDIC had completed PIAs on 43 of the 46 information systems it identified as containing information in an identifiable form. PIAs for the remaining systems, as well as efforts to identify additional systems, were planned or underway at the close of our audit.

System and Services Acquisition

System and services acquisition involves allocating resources to protect information systems, implementing an SDLC methodology that addresses security, and including security requirements and/or specifications in systems acquisitions. System and services acquisition also involves developing systems documentation, enforcing software usage restrictions, and ensuring proper security engineering principles, configuration management, and testing in applications systems development projects.

---

[29] PIAs are required under the E-Government Act of 2002 as implemented by OMB's September 26, 2003 memorandum (M-03-22) entitled, *OMB Guidance for Implementing the Privacy Provision of the E-Government Act of 2002.* PIAs must address the type of information being collected from individuals; why the information is being collected; the intended use of the information; with whom the information will be shared; which notice or opportunities for consent would be provided to individuals regarding the information that is collected and how the information is shared; how the information will be secured; and whether a system of records is being created under the Privacy Act.

[30] Common security controls can be applied to one or more information systems.

[31] OMB defines "information in an identifiable form" as information in a system or on-line collection that directly identifies an individual (e.g., name, address, Social Security number or other identifying code, telephone number, e-mail address, etc.) or by which an agency intends to identify specific individuals in conjunction with other data elements.

Although we performed limited work in the area of system and services acquisition for this evaluation, we noted that the FDIC had established policies and procedures in key system and services acquisition areas. However, the FDIC needed to update Circular 1320.3, *Systems Development Life Cycle (SDLC) Version 3.0*, dated July 17, 1997, to be consistent with the FDIC's Rational Unified Process (RUP®) SDLC methodology established in 2004.[32] RUP® is a key control for ensuring that security is integrated into the life-cycle management of the FDIC's information systems.

Certification, Accreditation, and Security Assessments

The C&A of federal information systems is critical to securing the government's operations and assets. Certification involves the evaluation of an information system's management, operational, and technical security controls. Accreditation involves a senior agency official's authorization of an information system to operate, including acceptance of any residual risk associated with operating the system. ST&E is performed in support of C&A. OMB requires agencies to certify and accredit their information systems in accordance with federal security policies, standards, and guidelines. In addition, the OMB has placed a high priority on fully certifying and accrediting federal information systems.

In our-prior year security evaluation, we reported that the FDIC had established C&A program controls that were generally consistent with NIST security standards and guidelines but that improvements in some areas were needed. In February 2006, we issued a separate audit report recognizing the significant strides that the FDIC had made in developing its C&A program in response to emerging NIST requirements.[33] Our report also identified opportunities for the FDIC to further strengthen its C&A policies, procedures, and guidelines. In June 2006, DIT revised its risk management methodology to achieve cost-efficiencies in its C&A processes and ensure alignment with NIST-recommended security standards and guidelines. At the close of our evaluation, DIT was working to complete revisions to its IT security risk management methodology, including the development of procedures for performing (a) continuous monitoring of systems after accreditation and (b) contingency planning of its information systems. Such procedures are critical to ensuring risk-based and cost-effective security oversight of the FDIC's information systems.

In our prior-year security evaluation, we reported that the FDIC had fully certified and accredited one system and granted Interim Authorizations to Operate (IATO) for four additional systems. At the close of our current year evaluation, the FDIC had fully certified and accredited 14 of its 15 major applications and general support systems consistent with NIST security standards and guidelines. Such an accomplishment is notable. Nevertheless, more work remains to ensure that the remaining 152 FDIC information systems subject to C&A, some of which process sensitive agency information, are certified and accredited.

---

[32] RUP® is a vendor-provided methodology that helps ensure security is considered and implemented throughout the SDLC, which includes multiple check points for security testing.

[33] *The FDIC's Security Certification and Accreditation Program*, dated February 2006 (Report No. 06-007).

Additionally, DIT needed to modify its POA&M procedures to ensure that all relevant IT security deficiencies are incorporated into or accompany system-level POA&Ms, including deficiencies identified in GAO, OIG, and any other security reviews. Current C&A guidelines provide that only ST&E weaknesses[34] are recorded and tracked in system-level POA&Ms.[35] Our analysis of the LAN/WAN and mainframe POA&Ms confirmed that DIT had not included in system-level POA&Ms those deficiencies reported by the GAO. Such deficiencies are tracked separately in the FDIC's Internal Risks Information System. Our assessment of the LAN/WAN and mainframe POA&Ms found that ST&E weaknesses were being properly tracked through remediation. However, the inclusion or accompaniment of GAO or OIG findings within the system-level POA&M process would benefit the system owners as issues are aggregated, tracked centrally, and reviewed monthly as part of the FDIC's existing C&A procedures.

[34] An ST&E weakness is a system deficiency identified during a security assessment of the system security controls.

[35] OMB's October 17, 2001 memorandum (M-02-01) entitled, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, (and subsequent guidance) states that POA&Ms should reflect consolidation with, or be accompanied by, other agency plans to correct security weaknesses found during any review done by, for, or on behalf of the agency. Such reviews include GAO audits, financial system audits, FISMA reviews, and critical infrastructure vulnerability assessments. The applicability of OMB's POA&M-related memoranda, including M-02-01, is under consideration by the FDIC.

OPERATIONAL CONTROLS

Operational controls are the safeguards and countermeasures for an information system that are primarily implemented and executed by individuals (as opposed to information systems). Operational controls include nine control families: *Personnel Security, Physical and Environmental Protection, Contingency Planning, Configuration Management, Maintenance, System and Information Integrity, Media Protection, Incident Response,* and *Awareness and Training*. In summary, we found the controls that we tested in the areas of *Contingency Planning, Incident Response,* and *Awareness and Training* were effective. However, the controls we tested related to *Personnel Security, Physical Security and Environmental Protection, Configuration Management, Maintenance, System and Information Integrity,* and *Media Protection* warrant management attention.

Personnel Security

Personnel security involves the implementation of policies, procedures, and practices for assigning risk designations to positions, screening individuals for those positions, and ensuring that systems access is terminated when personnel leave an agency or are transferred. Personnel security also involves ensuring that appropriate access agreements such as nondisclosure and conflict of interest agreements are in place for employees and contractors and implementing a formal sanctions process for personnel that fail to comply with security policies and procedures.

The FDIC has established personnel-related policies and procedures for its employees and contractors that were generally adequate. As part of our evaluation, we judgmentally selected 30 current FDIC employees and verified that their background investigations were commensurate with their positions' risk designations reflected in the FDIC's Corporate Human Resources Information System. In addition, we judgmentally selected 15 recently-separated FDIC employees and verified that a completed *Pre-Exit Clearance Record for Employees* was on file for all 15 former employees.[36] In addition, DOA was working to address two open recommendations related to personnel security that were contained in a prior OIG audit report.[37]

A key area of risk related to personnel security involves contractor confidentiality agreements. The FDIC's *Acquisition Policy Manual* (APM) requires contractors and subcontractors to complete a *Contractor Confidentiality Agreement* when such employees have access to confidential information, work on-site at the FDIC, or have

[36] FDIC Circular 2150.1, *Pre-Exit Clearance Procedures for FDIC Employees*, defines procedures for safeguarding FDIC-owned property and interests when employees leave the Corporation. A key component of these procedures is Form 2150/01, *Pre-Exit Clearance Record for Employees*, which contains a checklist of items that must be completed as part of the employee's pre-exit clearance process.

[37] In our March 30, 2004 Audit Report No. 04-016 entitled, *FDIC's Personnel Security Program*, we recommended, among other things, that the FDIC (a) review employees in moderate-risk level positions to ensure that appropriate background investigations have been performed and (b) re-assess low-risk-level employee positions having access to sensitive data in major applications to ensure that background investigations are completed for these employees commensurate with their access privileges.

access to FDIC systems. Confidentiality agreements are intended to provide the FDIC added assurance that contractors will properly safeguard confidential information in their custody. We judgmentally selected 30 current contractor employees who we determined would require a confidentiality agreement and found that the agreements for 10 such employees either had not been completed or could not be located. Additionally, we reported weaknesses related to contractor and subcontractor confidentiality agreements in our August 2006 Audit Report No. 06-016 entitled, *Controls Over the Disposal of Sensitive FDIC Information by Iron Mountain, Inc*. The FDIC needed to strengthen controls over contractor confidentiality agreements to ensure the requirement to protect sensitive information is fully understood by cognizant parties and to promote accountability.

Physical Security and Environmental Protection

Physical and environmental protection relates to those security measures aimed at safeguarding information systems, facilities, and related supporting infrastructures from threats. Such security measures include, but are not limited to, physical access controls, emergency power and lighting, fire protection, and temperature and humidity controls. Such measures also include procedures for the delivery and removal of systems hardware, firmware, and software to and from facilities.

The FDIC has established corporate-wide physical security program policies and procedures. However, we identified several physical security control weaknesses during our evaluation. In most cases, DOA either had addressed or was taking action to address these weaknesses.

On July 11, 2006, we conducted a walkthrough of the FDIC's Virginia Square facility and identified a significant amount of documented sensitive information stored in unsecured filing cabinets located in common areas. For example, we found documentation containing information in an identifiable format (i.e., employee names and Social Security numbers), attorney-client privileged information, investigation results, and a sensitive discussion of recent litigation. During our audit, we advised DIT of the need to secure this information. A DIT official stated that DIT was taking prompt corrective action. Our walkthrough also identified six unsecured mechanical rooms housing the building's heating, ventilation, and air conditioning systems; water supply; and electrical equipment. A DOA official indicated that card readers had originally been planned for the entrances to the mechanical rooms and that installing locks now (as an interim measure) would make installing the card readers more difficult. Prior to the close of our field work, DOA had secured all six mechanical rooms.

On July 18, 2006, we performed a site visit of the FDIC's new disaster recovery data center and noted areas where access to facilities could be better controlled. A DOA official indicated that DOA was aware of the issues and that improvements were planned. With regard to physical access to the FDIC's Virginia Square Data Center, DOA was generating reports of employee and contractor access to the center and providing the reports to DIT for review and analysis. However, a DIT official indicated that the data center access reports are reviewed on an ad hoc basis. The FDIC needs to establish a

procedure for regularly reviewing these reports for potential security incidents consistent with NIST-recommended security practices.

In addition, we were unable to determine whether selected employees and contractors with access to the FDIC's Washington, D.C., area facilities had appropriate access authorizations because access authorization documentation was not readily available. We judgmentally sampled 30 current employees and contractors and attempted to verify whether FDIC Form 1620/01, *Employee/Contractor Identification Card Request*, had been completed and approved.[38] A DOA official provided us with access forms for 7 of the 30 employees and contractors but indicated that locating the remaining authorizations would require time and research. At the close of our evaluation, we had not been provided with access forms for the remaining 23 employees and contractors.

We noted that the FDIC had implemented and regularly tested environmental controls within the Virginia Square Data Center that are vital to ensuring the availability of critical hardware and software. Such controls include cooling systems to maintain appropriate temperature levels, fire detection and suppression to provide life-saving services, uninterrupted power to maintain a clean power supply, and diesel generators to provide backup power.

Contingency Planning

Effective contingency planning and testing is essential to mitigate the risk of system and service unavailability. Contingency planning involves developing and implementing system contingency plans that address roles, responsibilities, and activities associated with restoring a system after a disruption or failure. Such planning also involves training personnel, testing systems, performing system backups, and establishing alternative processing sites.

The FDIC has established a corporate contingency planning program policy[39] and a business recovery plan template that are consistent with NIST guidelines. In addition, the FDIC has updated its business impact analysis (BIA) to validate its current IT recovery priorities. Further, the mainframe and LAN/WAN recovery plans were generally consistent with NIST security guidelines; however, we did note some minor discrepancies.[40] In early March 2006, the FDIC consolidated its IT disaster recovery operations at a new location. Later that same month, the FDIC conducted an IT disaster

[38] FDIC Circular 1610.1, *FDIC Physical Security Program*, states that administrative officers are responsible for approving form FDIC 1620/01 for all new employees, interns, detailees, and others who require an FDIC identification badge. Once completed and approved, the form is forwarded to DOA Corporate Services Branch.

[39] Circular 1360.13, *DIRM's* [Division of Information Resources Management] *Contingency Planning Program Policy*, dated November 22, 2004. DIT formerly operated under the title of DIRM.

[40] The FDIC did not incorporate the BIA into the overall business continuity documentation for reference purposes in the event of plan activation as recommended by NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*. In addition, the mainframe recovery plan did not address NIST-recommended security controls related to training, exercise and testing schedules, and plan maintenance.

recovery test of its mission-critical applications and general support systems. The FDIC has developed plans to address the issues it identified during the March 2006 test and conducted a limited disaster recovery test in June 2006 to determine whether certain issues had been adequately addressed. We plan to conduct a more detailed analysis of the FDIC's IT disaster recovery capability in a future audit assignment.

Configuration Management

Key to ensuring the confidentiality, integrity, and availability of any information system is implementing structured processes for managing the inevitable changes that will occur during the system's life cycle. Such processes, collectively referred to as configuration management, include evaluating, authorizing, testing, tracking, reporting, and verifying both hardware- and software-related changes.

The FDIC has documented guidelines for ensuring the proper configuration of its routers and switches and has performed monthly vulnerability scans of this equipment to ensure that security weaknesses have been identified, analyzed, corrected, and documented. In addition, routers and switches that we selected for review were configured consistent with the FDIC's documented baseline configurations. In July 2006, the FDIC significantly improved the configuration management of its corporate firewalls by implementing a formal change management tool.[41] Prior to July 2006, firewall rule set changes were handled through e-mail and did not require formal approvals. Implementing the change management tool was a notable improvement, but the corporate firewalls do not have documented baseline configurations. The baseline configuration coupled with a change control process ensure that the current configuration for hardware and software is accurate. Such accuracy is critical for decision making regarding the need to implement security patches or functionality upgrades. Once these firewall configurations are established, the FDIC should use an automated tool to analyze the configuration of its firewalls, such as the tool used for analyzing the configuration of the FDIC's routers and switches.

With regard to the mainframe, we identified a powerful program that could have allowed any mainframe programmer to bypass all security controls for the system. We considered this vulnerability to be serious in nature and brought it to DIT's attention, and the program was promptly removed from the system. The FDIC needs to take additional measures to ensure that powerful programs on the mainframe are strictly controlled. Such measures could include maintaining a current and complete listing of such programs, tracking changes to such programs, and periodically reviewing the integrity of such programs.

Although the FDIC uses the CA-Endeavor® automated configuration management tool[42] to process mainframe application software changes, the FDIC does not use a

[41] The FDIC implemented Remedy to track requests through system life-cycle stages (i.e., request, approval, implementation, and closure).

[42] CA-Endeavor® is a software product providing automated support for change, configuration, or version control.

configuration management tool to process mainframe system software[43] changes. The FDIC handles mainframe system software changes (including in-house-developed source code) manually. Change management tools provide added assurance that software is properly controlled and that changes are properly recorded, tracked, approved, and reported. For example, CA-Endeavor® interfaces with the mainframe's access control software to secure source code and object code libraries on the mainframe from unauthorized changes. Updates to source code libraries require system and application programmers to "check-in" their code, request approval, and migrate software changes to production system libraries.

Maintenance

Maintenance involves scheduling, performing, and documenting preventative and regular maintenance on the components of information systems in accordance with manufacturer or vendor specifications and/or organization requirements. Maintenance also involves approving, controlling, and monitoring maintenance tools and activities.

The FDIC has established policies and procedures for maintaining its information system components. The FDIC maintains current operating system software for its routers, switches, and firewalls and has established full-service contracts with vendors and vendor-certified partners to support its LAN/WAN. In addition, the FDIC maintains vendor-supported operating system software on the mainframe. However, the vendor has announced plans to discontinue its support of the current operating system software on the FDIC's mainframe, beginning in March 2007. Accordingly, the FDIC must determine whether to upgrade the mainframe's operating system software or use it without vendor support. In addition, the FDIC is in the process of acquiring a new network intrusion detection system (IDS) solution because vendor support for its current IDS solution has been discontinued. The risk of loss of vendor support to critical software must be carefully considered in updating the FDIC's EA and proceeding with technical solutions.

System and Information Integrity

System and information integrity controls include security controls for identifying, reporting, and correcting information system flaws. Such flaws can be discovered through the agency's system security assessments, continuous monitoring, or software vendors that recommend the implementation of software patches, service packs, or hotfixes to their software. System and information integrity control also involves the deployment of virus protection and intrusion detection mechanisms to protect the agency's IT operations and the implementation of controls for ensuring the accuracy, completeness, and validity of information.

The FDIC established policies and procedures designed to ensure the integrity of its systems and information. The FDIC has deployed anti-virus and IDS technologies to

[43] Examples of system software for the mainframe include Multiple Virtual Storage, Virtual Telecommunications Access Method, and Job Entry Subsystems.

protect its network operations. In addition, the FDIC has established performance measures to monitor the deployment of its software patches against pre-established timeframes. With regard to the mainframe, we noted that system security software was not configured to verify the identity of on-line programs to prevent spoofing—concealing a program with malicious intent by imitating a legitimate program. Spoofing a program could allow a programmer to gain another user's identification (ID) and password.

In its September 2006 report entitled, *Responses to Security-Related Questions in OMB's Fiscal Year 2006 Reporting Instructions for FISMA and Agency Privacy Management*, KPMG LLP (KPMG)[44] noted that the FDIC had generally implemented timely security patches for its UNIX® Solaris™ server and Microsoft for Windows® server and desktop operating systems. However, DIT was working to address a problem it had identified relating to the Windows® automated patch delivery tool. Specifically, at the end of our fieldwork, about 150 desktops and servers (combined) on the network had not been properly configured to automatically receive and install software patches. Additionally, we identified six Windows servers for which several required patches had not been installed. We brought these servers to DIT's attention. Subsequently, a DIT official advised us that DIT had retired two of the six servers and installed patches on the remaining four. We plan to report the effectiveness of the corrective actions in our separate report to the CIO.

Media Protection

Media protection involves those security controls related to controlling access to hard-copy and electronic media, labeling media consistent with its sensitivity, and ensuring media storage is secured. Media protection also involves safeguarding the transportation of media and ensuring that appropriate controls are in place when sanitizing and disposing of media.

The FDIC has established corporate policies and procedures for managing and disposing of sensitive records created or acquired in the course of conducting business.[45] Additionally, the FDIC was working to develop a corporate policy describing rules for storing, using, and disposing of sensitive FDIC data throughout its life cycle in response to OMB Memoranda M-06-16, *Protection of Sensitive Agency Information*, dated June 23, 2006; and M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, dated July 12, 2006. Issuance of this policy is key to providing security for sensitive agency information. DIT plans to address the labeling of sensitive data in the new policy. In Audit Report No. 06-016, we reported that the FDIC had established key controls for ensuring the secure disposal of sensitive information by its records management contractor. However, the FDIC needed to improve its oversight of the records management contractor to ensure that the controls for safeguarding the disposal of sensitive information had been effectively implemented.

[44] KPMG, under contract to the FDIC OIG, performed the audit work for this report.

[45] FDIC Circulars 1210.18, *FDIC Records Management Program*; 1210.1, *FDIC Records Retention and Disposal Schedule*; and 1210.4, *Records Disposition*.

Incident Response

FISMA requires that agency information security programs include procedures for detecting, reporting, and responding to security incidents. Implementing an effective incident response capability involves consideration of many factors, including training and detection, analysis, containment, eradication, reporting, and recovery from security incidents.

As indicated in our 2005 security evaluation report, the FDIC has continued to maintain a computer security incident response capability consistent with SP 800-61, *Computer Security Incident Handling Guide*. The FDIC has provided regular training to its Computer Security Incident Response Team members and has prepared procedure manuals containing detailed guidance for the prevention, detection, analysis, response, recovery, and reporting of security incidents.

Awareness and Training

FISMA requires federal agencies to provide security awareness training to users of agency information systems and requires agency CIOs to ensure proper oversight and training of personnel with significant information security responsibilities. In addition, federal regulations require agencies to develop a security awareness and training plan, identify employees with significant security responsibilities, and provide role-specific training in accordance with NIST standards and guidance.[46]

The FDIC has continued its prior-year practices of requiring (1) network users to complete an annual security awareness orientation,[47] (2) major application users to complete application-specific security awareness training, and (3) general support system technicians and managers to complete system-specific security training. Further, DIT has developed a formal training plan to ensure its staff with significant information security responsibilities receive appropriate security training for the type of work they perform. While these actions were positive, the FDIC needed to strengthen its procedures for ensuring that new network users complete required security awareness training on a timely basis. We randomly selected 45 network user accounts that had been created in 2006 for new FDIC employees and contractors. We found that 13 users (28 percent) had not completed the awareness orientation within the 5-day period defined in Circular 1360.16. We spoke with a DIT official about these users and learned that there can be

[46] The FDIC has determined that 5 Code of Federal Regulations Part 930, Subpart C, *Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems*, applies to the Corporation.

[47] Circular 1360.16, *Mandatory Information Security Awareness Training*, requires users of the FDIC's network to complete an annual Web-based information security awareness orientation. The circular states that new employees shall log on and review the FDIC Information Security Awareness Web site and orientation as soon as their network access is granted. Failure to do so within 5 working days of receiving a network ID may result in revoking employee and contractor access to FDIC systems and applications. The orientation includes information about laws, regulations, and policies related to computer security; rules of behavior for systems and major applications; tips on effective security; and links to additional sources of information.

legitimate reasons why a new network user may not take the awareness training within the 5-day period.[48] However, the DIT official acknowledged that improved procedures are needed to assist division and office ISMs in ensuring that new network users complete the security awareness training in a timely manner.

[48] For example, a user may not log into the network within 5 days of the creation of the user's account.

TECHNICAL CONTROLS

Technical controls are the safeguards or countermeasures for an information system that are primarily implemented and executed by the system through mechanisms contained in the hardware, software, or firmware components of the system. SP 800-53 separates technical controls into four control families: *Identification and Authentication*, *Access Control*, *Audit and Accountability*, and *System and Communications Protection*. In summary, we found that the controls we tested in the area of *Identification and Authentication* are effective. However, the controls tested in the areas of *Access Control* and *Audit and Accountability* warrant management attention. Due to our limited testing of *System and Communications Protection* controls, we did not assess this control family as part of our current-year work.

Identification and Authentication

Identification and authentication are security measures designed to prevent unauthorized individuals or processes from accessing information systems and data. FIPS PUB 201, *Personal Identity Verification of Federal Employees and Contractors*, and associated publications establish standards and requirements for the identity verification of federal employees and contractors and for personal identity verification (PIV) credentials to be issued.[49] OMB has directed agencies to deploy products and operational systems to issue identity credentials meeting the FIPS PUB 201 standard by October 27, 2006. Individual identities can be authenticated using various means, such as passwords, card tokens, biometrics, or some combination thereof. Devices can be identified and authenticated using shared known information, such as a Media Access Control address and an organization authentication solution (i.e., IEEE 802.1x and Extensible Authentication Protocol).

Generally, the FDIC implemented adequate policies, procedures, and practices for identifying and authenticating users of its LAN/WAN and mainframe. These controls included processes for systems access requests by users, management approval of systems access requests, and periodic re-authorizations of systems access privileges. With regard to the FDIC's efforts to implement a PIV system for its employees and contractors, the FDIC has contracted with a firm to obtain consulting and technical assistance. Due to uncertainties regarding how a PIV solution will be implemented, the FDIC had not yet developed a project plan or determined when it will have NIST-compliant processes for verifying the identity of its employees and contractors and issuing PIV identity credentials. We plan to evaluate the FDIC's efforts to address these processes as part of our 2007 FISMA evaluation work.

[49] NIST released FIPS PUB 201 in response to Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, on August 27, 2004. HSPD-12 requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification. The FDIC is not required to implement HSPD-12; however, the FDIC has decided to voluntarily comply with HSDP-12.

Access Control

Information system access controls (i.e., logical access controls) provide assurance that system resources can be accessed only by authorized users in authorized ways. Logical access controls provide a technical means of controlling the information users can read and copy, the programs they can execute, and the modifications they can make. Logical access controls also promote a key security principle known as "least privilege."[50]

The FDIC has established various policies and procedures that describe corporate-wide roles and responsibilities for managing access to its information systems and data.[51] In addition, DIT has identified improvements in the FDIC's access control program as one of its top priorities for 2006. At the time of our evaluation, DIT was performing an internal assessment of the FDIC's processes for granting user access to corporate information systems.

The FDIC has established and implemented a number of procedures for controlling access to its mainframe and LAN/WAN systems. However, improvements in some areas were needed. Regarding the LAN/WAN, we noted that access requests and approvals for routers and switches are handled through e-mail rather than through a centralized tool such as the FDIC's Access Authorization Security Application. The FDIC can enhance its LAN/WAN access control practices by using an automated tool. Regarding the mainframe, we identified two potential access control-related vulnerabilities as summarized below.

- An important mainframe security feature that prevents users from recovering deleted data sets was not enabled. Enabling this security feature would prevent users from recovering sensitive datasets that they may not be authorized to view. DIT officials indicated that they would evaluate the feasibility of implementing the security as part of a planned mainframe upgrade.

- Access restrictions designed to prevent a knowledgeable user from accessing powerful system software programs for unauthorized purposes, such as elevating their security privileges to access, modify, or delete program code, datasets, or other resources on the mainframe, were not consistent with mainframe security operating procedures. DIT officials indicated that they would review powerful system software programs to determine whether additional access restrictions should be implemented.

[50] Least privilege refers to the security objective of restricting user access to only those IT resources needed to perform official duties. Applying the principle of least privilege can mitigate damage to system resources resulting from accidents, errors, or unauthorized use.

[51] Such policies and procedures include, but are not limited to, Circular 1360.15, *Access Control for Automated Information Systems*, dated September 24, 2003; Circular 1370.1, *Periodic Review of Mainframe Resource Access*, dated July 17, 1995; the FDIC's *Access Control Procedures and Guidelines*, dated December 2002; and *Information Security Manager's (ISM) Guide*, dated August 2005.

In addition, we noted that the FDIC had not always restricted access to computer resources on the network consistent with the principle of least privilege. In March 2006, we reported that access to critical security software on the FDIC's laptop computers had not been appropriately restricted.[52] During our current-year FISMA evaluation work, we identified two contractor-maintained computers on the network that had not been restricted to prevent network users from accessing their operating system files or information stored on their hard drives, such as confidential bank data. Additionally, 1 of 10 network servers that we judgmentally selected for testing as part of our current year FISMA work had not been configured to prohibit users from controlling critical services. Specifically, any FDIC network user had the ability to start or stop critical services on the server, including e-mail services, antivirus software, and event logging. Although this vulnerable server appears to have been an isolated event, the issues discussed here collectively underscore the importance of conducting periodic reviews of network resources for least privilege.

We also found that the FDIC had established a corporate policy requiring its divisions and offices to monitor user access privileges for their information systems. However, the FDIC needs to develop an enterprise-wide approach for monitoring user access privileges commensurate with the sensitivity of the FDIC's information systems and data. Such an approach would help ensure that monitoring practices are commensurate with system sensitivity.

Regarding the encryption of sensitive information, OMB Memorandum M-06-16 recommends that departments and agencies encrypt all data on their mobile computers/devices that carry agency data unless the data is determined to be non-sensitive. The FDIC has implemented two separate software solutions for encrypting data on mobile laptop computers and removable media (including compact disks and flash drives). However, these solutions require manual intervention by users to encrypt sensitive data and files, limiting management's assurance that sensitive information is consistently encrypted on mobile computing devices. To address this limitation, the FDIC is currently pilot testing a new encryption solution that will secure all information in a manner transparent to users. The FDIC plans to deploy the new encryption solution based on the results of its pilot testing (currently scheduled for completion in November 2006).

Audit and Accountability

Audit trails, together with appropriate tools and procedures, promote key security-related objectives, such as detecting security violations, promoting individual accountability, and reconstructing auditable events. Audit and accountability involve generating audit records at a sufficient level of detail to establish the events that took place, sources of the events, and outcomes of the events. Audit and accountability also involve consideration of audit trail storage, processing, monitoring, analysis, reporting, protection, and retention.

[52] OIG Audit Report No. 06-012 entitled, *Security Controls Over the FDIC's Wireless Data Communications*, dated March 2006.

Although FDIC policy requires system developers to incorporate audit and accountability measures into new and existing information systems, the policy does not address audit logging and monitoring responsibilities for system owners.[53] In addition, the FDIC's RUP® SDLC methodology does not require system owners to define audit logging and monitoring requirements. Further, the FDIC has not developed procedures and guidelines to assist system owners in determining the circumstances under which system audit logs should be created, information that should be logged, and the methods available for logging and monitoring. Such procedural improvements are needed to ensure that the FDIC's practices for generating and monitoring audit logs are commensurate with the sensitivity levels of the systems and the data they processed.

Regarding the LAN/WAN, audit log information was centrally recorded and stored. DIT staff told us that they periodically review LAN/WAN audit logs. However, DIT had not documented procedures describing which audit log activities are reviewed, how often they are reviewed, or who reviews them or the types of actions that can be taken when potential security incidents are identified. Regarding the mainframe, the FDIC was taking action to log and monitor user access activities to ensure such activities were consistent with security policies and procedures. However, we identified five mainframe users with special privileges who were responsible for reviewing audit logs of their own activities. This approach did not provide for the appropriate separation of duties. We brought this weakness to DIT's attention during the evaluation, and prompt corrective action was taken.

Based on the results of our evaluation work in the areas of access control and audit and accountability, we concluded that management attention is warranted to ensure that appropriate risk-based security controls are in place and operating as intended.

System and Communications Protection

System and communications protection addresses a number of key security control measures including, but not limited to, ensuring that system functionality is appropriately segregated; communications are monitored, controlled, and protected; and that cryptographic operations (if used) are adequate.

We did not perform specific audit procedures related to system and communications protection because the majority of controls in this family pertain to general support systems not covered under our current-year evaluation. Such general support systems include the Voice/Video, Public Key Infrastructure, and Remote Access systems. We plan to evaluate system and communications protection security controls in future FISMA evaluations.

[53] Circular 1360.15, *Access Control for Automated Information Systems*.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of our review was 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. The scope of our work included a review of the FDIC's common controls and certain NIST SP 800-53 control families of the LAN/WAN and mainframe general support systems, as well as the FDIC's progress in meeting HSPD-12 provisions.

To accomplish our objective, we interviewed key DIT and program office personnel who had significant information security responsibilities. Also, we evaluated the FDIC's security-related policies, procedures, and guidelines and certain security-related documents and files, including C&A documentation, vulnerability assessments, IT services contracts, training records, and strategic and annual performance plans. We tested the FDIC common controls and the LAN/WAN and mainframe in order to determine the FDIC's compliance with its policies and procedures and federal guidelines. Appendix II lists the SP 800-53 controls included in the scope of our review.

We engaged KPMG to perform our assessment of the FDIC's common controls and LAN/WAN and mainframe system security controls. Our oversight of KPMG included evaluating the nature, timing, and extent of work described in KPMG's evaluation program, attending key meetings with KPMG, monitoring KPMG's work throughout the evaluation, and performing other procedures we deemed appropriate. In this manner, we assured ourselves that KPMG's work complied with generally accepted government auditing standards (GAGAS).

In the performance of our FISMA work, we leveraged security-related audit, review, and evaluation reports issued by the GAO and others, including the FDIC's OIG. To assure ourselves that we could leverage pertinent information contained in these reports, we performed appropriate procedures, such as obtaining an understanding of the methodologies, assumptions, and conclusions described therein.

In addition, our evaluation did not assess controls at depository institutions insured and regulated by the FDIC that routinely provide financial information to the Corporation. We performed our evaluation at the FDIC's Headquarters office and primary computer facility in Arlington, Virginia, and the new disaster recovery site during the period April through August 2006. Throughout our evaluation, we met with FDIC management to discuss our preliminary conclusions. We conducted our evaluation in accordance with GAGAS.

Internal Control

An explanation of the terms "internal control," "reasonable assurance," and "adequate security" is important to ensure a proper understanding of our approach and conclusions.

OMB Circular No. A-123 (OMB A-123), *Management's Responsibility for Internal Control*,[54] states:

> Internal Control—organization, policies, and procedures—are tools to help program and financial managers achieve results and safeguard the integrity of their programs.

Additionally, OMB A-123 states that reasonable assurance must be provided by internal control. The circular states:

> Internal control is an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

OMB A-130, Appendix III,[55] defines adequate security as security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or modification of or unauthorized access to information. This includes assuring that agency systems and applications provide appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls. The concept of adequate security is consistent with FISMA, which directs agency heads to provide information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access to, use, disclosure, disruption, modification, or destruction of information and information systems.

Government oversight agencies, such as GAO and OMB, and recognized standards-setting organizations such as NIST have identified fundamental management principles and controls needed to implement an effective information security program.[56] The controls were defined with the publication of FIPS PUB 200 and SP 800-53, and an assessment methodology was outlined in a draft assessment guide in SP 800-53A. SP 800-53 defines a minimum set of security controls for the non-national security systems of all federal agencies. These security controls are selected based on the potential impact that could occur to the agency should there be a loss of confidentiality,

---

[54] On December 21, 2004, OMB revised the circular, which became effective in fiscal year 2006, to strengthen requirements for conducting management's assessment of internal control over financial reporting and to emphasize the need for agencies to integrate and coordinate internal control assessments with other internal-control-related activities. The circular implements the FMFIA. This Act is applicable to the FDIC because of provisions in the Chief Financial Officers Act of 1990 regarding annual reporting by government corporations on their internal accounting and administrative control systems. The FDIC has determined that as long as it develops internal controls that are consistent with the goals of FMFIA, the FDIC will have met its legal obligations under the circular.

[55] OMB A-130, Appendix III, establishes minimum controls for federal automated information security programs. The FDIC has determined that portions of the circular apply to the FDIC, while other portions do not apply. The FDIC has also determined that OMB A-130, Appendix III, requires the FDIC to implement and maintain an information security program consistent with government-wide policies, standards, and procedures issued by OMB and the Department of Commerce.

[56] GAO Executive Guide, Information Security Management: *Learning From Leading Organizations*; OMB A-130, Appendix III; SP 800-14; SP 800-12; and SP 800-53.

integrity, or availability of the information or information system. The publication defines 17 management, operational, and technical security control families that are integral to securing any federal information system.

In addition to the SP 800-53 controls for securing systems, draft SP 800-100 describes other controls for agency-wide management of a security program. Based on our analysis of draft SP 800-100 and considering the FDIC's business and IT environment, we identified three additional security program control families, *Information Security Governance*, *Enterprise Architecture*, and *Capital Planning*. Table 3 lists the security control classes and related security control families.

Table 3: Security Control Classes and Families

Security Control Class	Security Control Family
Program	Information Security Governance
	Enterprise Architecture
	Capital Planning
Management	Risk Assessment
	Planning
	System and Services Acquisition
	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
	Physical and Environmental Protection
	Contingency Planning
	Configuration Management
	Maintenance*
	System and Information Integrity
	Media Protection*
	Incident Response
	Awareness and Training
Technical	Identification and Authentication
	Access Control
	Audit and Accountability*
	System and Communications Protection

Source: OIG analysis of NIST guidance.
*This control family was not included in prior OIG FISMA evaluations of the FDIC's information security program.

We assigned one of three assurance levels (reasonable assurance, limited assurance, and minimal/no assurance) when assessing the effectiveness of the information security program. We used OMB guidance to develop definitions for reasonable, limited, and minimal assurance (see Table 4).

Table 4: Information Security Program Assurance Levels

Reasonable Assurance	Indicates that the Corporation has established or implemented controls that were sufficient to provide reasonable, but not absolute, assurance of achieving adequate security over its information resources. Designations of reasonable assurance indicate that the FDIC has designed or implemented controls to ensure compliance with applicable statutory or regulatory requirements and that such controls maintained appropriate confidentiality, integrity, and availability of information resources.
Limited Assurance	Indicates that the Corporation has established controls that were partially complete or has implemented controls that were not always effective or operating as intended. Designations of limited assurance indicate that the FDIC was in partial compliance with applicable statutory or regulatory requirements and that control weaknesses existed in the confidentiality, integrity, or availability of information resources. Although mitigating controls may exist, control weaknesses may impede the FDIC's ability to achieve its security goals and objectives.
Minimal/No Assurance	Indicates that the Corporation has established few or no controls to provide assurance of adequate security or that existing controls were not operating as intended. Designations of minimal/no assurance indicate significant noncompliance with applicable statutory or regulatory requirements and serious control weaknesses relating to the confidentiality, integrity, or availability of information resources. Because mitigating controls were minimal or not present, the achievement of corporate security goals and objectives was impaired. Minimal/no assurance is indicative of weaknesses that merit the attention of the FDIC Chairman and Board of Directors.

Source: OIG analysis of OMB guidance.

The OIG changed its methodology from prior years to better conform to the emerging standards and guidance. Our current FISMA evaluation framework consists of assessing the program control class on an agency-wide basis and assessing management, operational, and technical control classes on a sample of systems. The assessment of control families is based on testing a sample of the controls that make up the family. We selected systems, control families, and individual controls for testing based on how important the system is to the FDIC, the control family is to the system, and the control is to the control family. We considered risk, costs, results of internal and external reviews, government-wide and FDIC initiatives and goals, the maturity of the security program, and other factors in selecting our samples. For fiscal year 2006, we sampled two general support systems—the mainframe and LAN/WAN. Appendix II identifies the security control families for which we performed limited testing of system-level controls.

In previous years, based on our analysis of long-standing requirements found in security-related statutes, policies, and guidance and considering the FDIC's business and IT environment, we identified 10 key management control areas associated with the FDIC's information security program. For each of the 10 management control areas, we provided an assessment in terms of the level of assurance that the management control provided adequate security over the FDIC's information resources. Using each of the 10 management control assessments as a basis and considering associated risk, we then assessed the Corporation's overall information security program and compared it to previous security evaluation results. In this manner, we were able to evaluate the FDIC's progress in strengthening its information security program and practices. However, we were unable to make a meaningful comparison of results from the prior and current annual evaluations due to differences in the nature and extent of control testing performed.

Laws and Regulations

We evaluated the FDIC's compliance with FISMA[57] and information-security-related laws, policies, procedures, standards, and guidelines (or provisions thereof) that had a direct and material impact on the FDIC's information security program and practices. Our evaluation focused primarily on FISMA and OMB A-130, Appendix III,[58] as criteria for the major elements of an effective information security program. Our evaluation also placed particular reliance on a number of statutes, policies, and guidance; including but not limited to:

- The E-Government Act of 2002[59]
- FMFIA[60]
- The Clinger-Cohen Act of 1996[61]
- The Government Performance and Results Act of 1993[62]

[57] FISMA, codified in pertinent part to titles 40 and 44, United States Code (U.S.C.), is similar to Title X of the Homeland Security Act of 2002 (Pub. L. No. 107-269), which also bears the name Federal Information Security Management Act of 2002. In signing the E-Government Act of 2002 into law, the President stated that the executive branch will construe the E-Government Act of 2002 as permanently superseding the Homeland Security Act of 2002 in those instances where both Acts prescribe different amendments to the same provisions of the U.S.C. Also, see 44 U.S.C. § 3549 regarding the effect of the E-Government Act on existing law.

[58] The FDIC has determined that portions of the Circular apply to the FDIC.

[59] The FDIC had determined that this statute, Title III of which contains FISMA, is legally binding on the FDIC.

[60] The FDIC has determined that portions of the FMFIA are applicable to the FDIC by reference in the Chief Financial Officers Act. In general, the goals of FMFIA are that agency obligations and costs comply with applicable law; assets are guarded against waste, loss, etc.; and revenue and expenditures are properly accounted for, so that reliable financial statements can be prepared.

[61] The FDIC has determined that the Clinger-Cohen Act does not apply to the FDIC. The Clinger-Cohen Act imposes obligations and responsibilities on "executive agencies" as defined in the Office of Federal Procurement Policy Act, which does not include the FDIC. However, the FDIC has indicated that it intends to follow the spirit of the Act.

- The Chief Financial Officers Act of 1990[63]
- The Privacy Act of 1974[64]
- 5 Code of Federal Regulations Part 930, Subpart C, *Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems*[65]
- HSPD–7, *Critical Infrastructure Identification, Prioritization, and Protection*[66]
- HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*[67]
- OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*[68]
- OMB Circular No. A-123, *Management Responsibility for Internal Control*[69]
- The following OMB security-related memoranda:
  - M-00-07, *Incorporating and Funding Security in Information Systems Investments*[70]
  - M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*[71]
  - M-03-22, OMB *Guidance for Implementing the Privacy Provision of the E-Government Act of 2002*[72]
  - M-06-15, *Safeguarding Personally Identifying Information*[73]
  - M-06-16, *Protection of Sensitive Agency Information*[74]
  - M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*[75]

---

[62] The Act 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.

[63] The FDIC has determined that the portions of this Act that are applicable to government corporations are also applicable to the FDIC.

[64] The Act, which is applicable to the FDIC, requires agencies to have appropriate administrative, technical and physical safeguards over the security and confidentiality of agency records

[65] The FDIC has determined that this provision applies to the FDIC.

[66] The FDIC has determined that HSPD-7 applies to the Corporation.

[67] According to OMB guidance for implementing HSPD-12, government corporations are encouraged to comply with the directive. The FDIC is voluntarily complying with this directive.

[68] This circular governs the federal budgeting process and contains requirements for identifying and tracking various agency costs. The FDIC prepares budgetary data for OMB's review but not approval.

[69] The FDIC has determined that this circular is applicable to the FDIC; specifically, as long as the FDIC's internal controls are consistent with the goals of the FMFIA, the FDIC will have met its obligations under this circular.

[70] The FDIC determined that this memorandum, which implements OMB Circular Nos. A-130 and A-11, was not applicable to the FDIC.

[71] The FDIC is reviewing this memorandum to determine its applicability to the FDIC.

[72] This memorandum implements section 208 of the E-Government Act, which applies to the FDIC.

[73] The applicability of this memorandum has not been determined; however, the FDIC has taken steps to implement it.

[74] The applicability of this memorandum, which deals with protecting information remotely accessed, has not been determined, but the FDIC has taken steps to implement it.

  - M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
- NIST FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*[76]
- NIST FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems.*[77]
- NIST FIPS PUB 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*[78]
- FDIC policies and procedures related to information security
- GAO's *Federal Information System Controls Audit Manual*[79]
- The following NIST Special Publications:[80]
  - 800-12, *An Introduction to Computer Security: The NIST Handbook*
  - 800-18, *Guide for Developing Security Plans for Information Technology Systems*
  - 800-30, *Risk Management Guide for Information Technology Systems*
  - 800-34, *Contingency Planning Guide for Information Technology Systems*
  - 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
  - 800-40, *Procedures for Handling Security Patches*
  - 800-47, *Security Guide for Interconnecting Information Technology Systems*
  - 800-50, *Building an Information Technology Security Awareness and Training Program*
  - 800-53, *Recommended Security Controls for Federal Information Systems*
  - 800-55, *Security Metrics Guide for Information Technology Systems*
  - 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*
  - 800-61, *Computer Security Incident Handling Guide*
  - 800-64, *Security Considerations in the Information System Development Life Cycle*
  - 800-65, *Integrating Security into the Capital Planning and Investment Control Process*

---

[75] This memorandum requires agencies to report computer incidents to a central federal incident-reporting center. Although legal applicability has not been determined, the FDIC has taken steps to implement this memorandum.

[76] Because the FDIC is not an executive agency for purposes of the publication, this publication is not legally applicable to the FDIC, but the FDIC follows its principles.

[77] The applicability of this publication has not been determined, but the FDIC intends to voluntarily comply with it.

[78] The FDIC is voluntarily complying with FIPS PUB 201.

[79] The manual provides guidance for reviewing information system controls that affect the integrity, confidentiality, and availability of computerized data.

[80] In general, these NIST SPs are, by their own terms, guidelines (rather than mandatory requirements) for agencies in implementing their IT operations. However, the current applicability of SP 800-53 to the FDIC has not been determined.

Computer-based Data, Performance Measures, and Fraud and Illegal Acts

We performed appropriate procedures to assure ourselves that computer-based data were valid and reliable when those data were significant to our evaluation findings and conclusions. Such procedures included verifying selected automated data to source documentation and corroborating automated data through interviews with appropriate FDIC personnel. In addition, we evaluated the adequacy and effectiveness of the FDIC's performance measures related to information security. Finally, we did not develop specific audit procedures to detect fraud and illegal acts because we did not consider fraud and illegal acts to be material to the evaluation objective. However, throughout our evaluation, we were sensitive to the potential for fraud, waste, abuse, and mismanagement.

APPENDIX II

NIST SP 800-53 CONTROLS TESTED

This appendix lists the recommended security controls for federal information systems from NIST SP 800-53 published in February 2005. We performed limited testing on a sample of controls identified in the Sample of Controls Tested column. We limited our tests based on the risk and feasibility within the FDIC's common control, mainframe, and LAN/WAN environments. We also tested program controls.

NIST SP 800-53 Control			Sample of Controls Tested
Family	**No.**	**Name**	
Management Control Class			
Risk Assessment (RA)	RA-1	Risk Assessment Policy and Procedures	X
	RA-2	Security Categorization	X
	RA-3	Risk Assessment	X
	RA-4	Risk Assessment Update	X
	RA-5	Vulnerability Scanning	X
Planning (PL)	PL-1	Security Planning Policy and Procedures	X
	PL-2	System Security Plan	
	PL-3	System Security Plan Update	
	PL-4	Rules of Behavior	X
	PL-5	Privacy Impact Assessment	X
System and Services Acquisition (SA)*	SA-1	System and Services Acquisition Policy and Procedures	X*
	SA-2	Allocation of Resources	
	SA-3	Life Cycle Support	
	SA-4	Acquisitions	
	SA-5	Information System Documentation	
	SA-6	Software Usage Restrictions	X*
	SA-7	User Installed Software	X*
	SA-8	Security Design Principles	
	SA-9	Outsourced Information System Services	
	SA-10	Developer Configuration Management	
	SA-11	Developer Security Testing	
Certification, Accreditation, and Security Assessments (CA)	CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	X
	CA-2	Security Assessments	X
	CA-3	Information System Connections	X
	CA-4	Security Certification	X
	CA-5	Plan of Action and Milestones	X
	CA-6	Security Accreditation	X
	CA-7	Continuous Monitoring	

APPENDIX II

NIST SP 800-53 Control			Sample of Controls Tested
Family	**No.**	**Name**	
Operational Control Class			
Awareness and Training (AT)	AT-1	Security Awareness and Training Policy and Procedures	X
	AT-2	Security Awareness	X
	AT-3	Security Training	X
	AT-4	Security Training Records	
Configuration Management (CM)	CM-1	Configuration Management Policy and Procedures	X
	CM-2	Baseline Configuration	X
	CM-3	Configuration Change Control	X
	CM-4	Monitoring Configuration Changes	X
	CM-5	Access Restrictions for Change	X
	CM-6	Configuration Settings	X
	CM-7	Least Functionality	X
Contingency Planning (CP)	CP-1	Contingency Planning Policy and Procedures	X
	CP-2	Contingency Plan	X
	CP-3	Contingency Training	X
	CP-4	Contingency Plan Testing	X
	CP-5	Contingency Plan Update	X
	CP-6	Alternate Storage Sites	X
	CP-7	Alternate Processing Sites	X
	CP-8	Telecommunications Services	X
	CP-9	Information System Backup	X
	CP-10	Information System Recovery and Reconstitution	X
Incident Response (IR)	IR-1	Incident Response Policy and Procedures	X
	IR-2	Incident Response Training	X
	IR-3	Incident Response Testing	
	IR-4	Incident Handling	X
	IR-5	Incident Monitoring	X
	IR-6	Incident Reporting	X
	IR-7	Incident Response Assistance	X
Maintenance (MA)	MA-1	System Maintenance Policy and Procedures	X
	MA-2	Periodic Maintenance	X
	MA-3	Maintenance Tools	
	MA-4	Remote Maintenance	
	MA-5	Maintenance Personnel	
	MA-6	Timely Maintenance	
Media Protection (MP)	MP-1	Media Protection Policy and Procedures	X
	MP-2	Media Access	X
	MP-3	Media Labeling	
	MP-4	Media Storage	X
	MP-5	Media Transport	X
	MP-6	Media Sanitization	X
	MP-7	Media Destruction and Disposal	

APPENDIX II

NIST SP 800-53 Control			Sample of Controls Tested
Family	**No.**	**Name**	
Physical and Environmental Protection (PE)	PE-1	Physical and Environmental Protection Policy and Procedures	X
	PE-2	Physical Access Authorizations	X
	PE-3	Physical Access Control	X
	PE-4	Access Control for Transmission Medium	
	PE-5	Access Control for Display Medium	
	PE-6	Monitoring Physical Access	X
	PE-7	Visitor Control	X
	PE-8	Access Logs	X
	PE-9	Power Equipment and Power Cabling	X
	PE-10	Emergency Shutoff	X
	PE-11	Emergency Power	X
	PE-12	Emergency Lighting	X
	PE-13	Fire Protection	X
	PE-14	Temperature and Humidity Controls	X
	PE-15	Water Damage Protection	X
	PE-16	Delivery and Removal	
	PE-17	Alternate Work Site	X
Personnel Security (PS)	PS-1	Personnel Security Policy and Procedures	X
	PS-2	Position Categorization	X
	PS-3	Personnel Screening	X
	PS-4	Personnel Termination	X
	PS-5	Personnel Transfer	X
	PS-6	Access Agreements	X
	PS-7	Third-Party Personnel Security	X
	PS-8	Personnel Sanctions	
System and Information Integrity (SI)	SI-1	System and Information Integrity Policy and Procedures	X
	SI-2	Flaw Remediation	X
	SI-3	Malicious Code Protection	X
	SI-4	Intrusion Detection Tools and Techniques	X
	SI-5	Security Alerts and Advisories	X
	SI-6	Security Functionality Verification	
	SI-7	Software and Information Integrity	
	SI-8	Spam and Spyware Protection	X
	SI-9	Information Input Restrictions	
	SI-10	Information Input Accuracy, Completeness, and Validity	
	SI-11	Error Handling	
	SI-12	Information Output Handling and Retention	

APPENDIX II

NIST SP 800-53 Control			Sample of Controls Tested
Family	**No.**	**Name**	
Technical Control Class			
Identification and Authentication (IA)	IA-1	Identification and Authentication Policy and Procedures	X
	IA-2	User Identification and Authentication	X
	IA-3	Device Identification and Authentication	
	IA-4	Identifier Management	X
	IA-5	Authenticator Management	X
	IA-6	Authenticator Feedback	X
	IA-7	Cryptographic Module Authentication	
Access Control (AC)	AC-1	Access Control Policy and Procedures	X
	AC-2	Account Management	X
	AC-3	Access Enforcement	X
	AC-4	Information Flow Enforcement	
	AC-5	Separation of Duties	
	AC-6	Least Privilege	X
	AC-7	Unsuccessful Login Attempts	X
	AC-8	System Use Notification	X
	AC-9	Previous Logon Notification	
	AC-10	Concurrent Session Control	
	AC-11	Session Lock	X
	AC-12	Session Termination	X
	AC-13	Supervision and Review – Access Control	
	AC-14	Permitted Actions w/o Identification or Authentication	X
	AC-15	Automated Marking	
	AC-16	Automated Labeling	
	AC-17	Remote Access	X
	AC-18	Wireless Access Restrictions	
	AC-19	Access Control for Portable and Mobile Systems	
	AC-20	Personally Owned Information Systems	
Audit and Accountability (AU)	AU-1	Audit and Accountability Policy and Procedures	X
	AU-2	Auditable Events	X
	AU-3	Content of Audit Records	X
	AU-4	Audit Storage Capacity	X
	AU-5	Audit Processing	X
	AU-6	Audit Monitoring, Analysis, and Reporting	X
	AU-7	Audit Reduction and Report Generation	
	AU-8	Time Stamps	X
	AU-9	Protection of Audit Information	X
	AU-10	Non-repudiation	
	AU-11	Audit Retention	X

NIST SP 800-53 Control			Sample of Controls Tested
Family	**No.**	**Name**	
System and Communications Protection (SC)*	SC-1	System and Communications Protection Policy and Procedures	X*
	SC-2	Application Partitioning	
	SC-3	Security Function Isolation	
	SC-4	Information Remnants	
	SC-5	Denial of Service Protection	
	SC-6	Resource Priority	
	SC-7	Boundary Protection	
	SC-8	Transmission Integrity	
	SC-9	Transmission Confidentiality	X*
	SC-10	Network Disconnect	
	SC-11	Trusted Path	
	SC-12	Cryptographic Key Establishment and Management	
	SC-13	Use of Validated Cryptography	
	SC-14	Public Access Protections	
	SC-15	Collaborative Computing	
	SC-16	Transmission of Security Parameters	
	SC-17	Public Key Infrastructure Certificates	
	SC-18	Mobile Code	
	SC-19	Voice Over Internet Protocol	

Source: KPMG and OIG compilation of controls tested.

*These control families and controls were included in our survey work; however, the scope of our work was not sufficient for us to provide an assessment of the control family.

ACRONYMS

Acronym	Definition
APM	*Acquisition Policy Manual*
BCP	Business Continuity Plan
BIA	Business Impact Analysis
C&A	Certification and Accreditation
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIRC	Capital Investment Review Committee
COBIT®	Control Objectives for Information and related Technology
COO	Chief Operating Officer
CPIM	Capital Planning and Investment Management
DIRM	Division of Information Resources Management
DIT	Division of Information Technology
DOA	Division of Administration
DOF	Division of Finance
EA	Enterprise Architecture
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act
FMFIA	Federal Managers Financial Integrity Act
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
HSPD	Homeland Security Presidential Directive
IATO	Interim Authorization to Operate
IBM	International Business Machines
ID	Identification
IDS	Intrusion Detection System
IG	Inspector General
ISM	Information Security Manager
ISS	Information Security Staff
IT	Information Technology
KPMG	KPMG LLP
LAN/WAN	Local Area Network/Wide Area Network
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget

Acronym	Definition
PIA	Privacy Impact Assessment
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
RUP®	Rational Unified Process®
SDLC	System Development Life Cycle
SP	Special Publication
ST&E	Security Testing and Evaluation
U.S.C.	United States Code

APPENDIX IV

GLOSSARY OF TERMS

Term	Definition
Access Controls	The ability to ensure that system resources can be accessed only by authorized users in authorized ways.
Adequate Security	Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Audit Trail	An audit trail is a series of records of computer-related events about an operating system, an application, or user activities. An information system may have several audit trails, each devoted to a particular type of activity. The terms audit trail and audit log are used synonymously in this report.
Auditable Event	An event is any action that happens on a computer system. Examples include logging into a system, executing a program, and opening a file.
Biometrics	One of various technologies that utilize behavioral or physiological characteristics to determine or verify identity. For example, a fingerprint scan is a commonly-used biometric.
Firmware	The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution.
Hotfixes	A hotfix is a single, cumulative package that includes one or more files that are used to address a problem in a product. Hotfixes address a specific customer situation and may not be distributed outside the customer organization.
Least Privilege	Refers to the practice of restricting a user's access to only those resources needed to perform official duties.
Log	A log is a record of the events occurring within an organization's systems and networks. Logs are composed of entries that contain information related to a specific event that occurred within a system or network.
Mainframe Dataset	The term dataset is used to refer to files on an IBM mainframe computer, typically stored on a direct-access storage device or magnetic tape. The term pertains to IBM mainframe operating systems.
National Institute of Standards and Technology (NIST)	A non-regulatory federal agency within the Department of Commerce's Technology Administration. As part of its responsibilities, NIST develops and publishes technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive, but unclassified, information in federal computer systems.
Object Code	Software program instructions compiled (translated) from source code into machine-readable formats.
Routers and Switches	A router is a computer networking device that forwards data packets toward their destinations through a process known as routing. A network switch is a computer networking device that connects network segments.
Source Code	A set of programming language instructions that must be translated to machine instructions before the program can run.

Term	Definition
Test Scripts	Test scripts constitute those series of actions, keystrokes, tabs, mouse clicks, etc. used to navigate through a single screen or a series of screens in an application.