Office of Inspector General

September 2005
Report No. 05-031

FDIC's Information Technology Configuration Management Controls Over Operating System Software

Office of Audits

oig

Office of Audits

OIG

Background and Purpose of Audit

The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) contracted with International Business Machines (IBM) Business Consulting Services to audit and report on the effectiveness of the FDIC's configuration management controls over operating system software. The results of this audit support the OIG in fulfilling its evaluation and reporting responsibilities under the Federal Information Security Management Act.

Configuration management is a critical control for ensuring the integrity, security, and reliability of information systems. Absent a disciplined process for managing software changes, management cannot be assured that systems will operate as intended, that software defects will be minimized, and that configuration changes will be made in an efficient and timely manner.

The objective of the audit was to determine whether the FDIC had established and implemented configuration management controls over its operating system software that were consistent with federal standards and guidelines and industry-accepted practices.

To view the full report, go to www.fdicig.gov/2005reports.asp

Report No. 05-031
September 2005

FDIC's Information Technology Configuration Management Controls Over Operating System Software

Results of Audit

The FDIC had established and implemented a number of configuration management controls over its operating system software that were consistent with federal standards and guidelines and industry-accepted practices. Such controls included a software patch management policy, a change control board, and periodic scanning of operating system software configurations. These actions were positive; however, control improvements were needed. Specifically, the FDIC needed to establish an organizational policy and system-specific procedures to ensure proper configuration of operating system software. The FDIC also needed to standardize and integrate the recording, tracking, and reporting of operating system software configuration changes to the extent practical.

Recommendations and Management Response

IBM recommends that the FDIC:

- establish an organizational policy that defines roles, responsibilities, and overall principles and management expectations for performing configuration management of operating system software;
- develop configuration management plan(s) that include system-specific procedures for managing the configuration of operating system software;
- ensure that the certification and accreditation of the FDIC's general support systems incorporate an evaluation and testing of the configuration management policy and plan(s) referenced above;
- fully document the minimum required configuration settings for the operating systems covered in this review, and develop procedures to ensure that changes to baseline configuration settings are documented; and
- standardize and integrate the recording, tracking, and reporting of configuration changes within and across operating system software platforms to the maximum extent practical.

FDIC management generally agreed with the report's recommendations and has either initiated or plans to initiate actions to address them.

Federal Deposit Insurance Corporation
801 17th Street NW, Washington, DC 20434

Office of Audits
Office of Inspector General

DATE: September 8, 2005

MEMORANDUM TO: Michael E. Bartell
Chief Information Officer and
Director, Division of Information Technology

FROM: Russell A. Rau [Original signed by Stephen M. Beard for Russell A. Rau]
Assistant Inspector General for Audits

SUBJECT: *FDIC's Information Technology Configuration Management Controls Over Operating System Software*
(Report No. 05-031)

Enclosed is a copy of a report completed by the independent professional services firm of International Business Machines (IBM) Business Consulting Services. The firm's report is presented as Part I of this document.

The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) contracted with IBM to audit and report on the effectiveness of the FDIC's configuration management controls over operating system software. The results of this audit support the OIG in fulfilling its evaluation and reporting responsibilities under the Federal Information Security Management Act of 2002. The objective of the audit was to determine whether the FDIC had established and implemented configuration management controls over its operating system software that were consistent with federal standards and guidelines and industry-accepted practices. The audit focused on four of the FDIC's operating system software platforms used to support sensitive and mission-critical business applications. This report provides recommendations to strengthen configuration management controls over the FDIC's operating system software.

Our evaluation of your response, a summary of your response and the status of corrective actions, and your response in its entirety is contained in Part II of this report. The response adequately addressed the recommendations in the report. We consider the report's recommendations to be resolved, but they will remain undispositioned and open for reporting purposes until we have determined that agreed-to corrective actions have been completed and are effective.

Table of Contents

Part I:

Report by International Business Machines (IBM) Business Consulting Services

FDIC's Information Technology Configuration Management Controls Over Operating System Software I-1

Part II:

Corporation Comments and OIG Evaluation II-1

Management Response to Recommendations II-4

Corporation Comments II-6

Part I

Report by IBM Business Consulting Services

IBM Business Consulting Services

FDIC's Information Technology Configuration Management Controls Over Operating System Software

Report No. 05-031

Prepared for the Federal Deposit Insurance Corporation Office of Inspector General

Submitted by: IBM Business Consulting Services
Security, Privacy, & Wireless
12902 Federal Systems Park Drive
Fairfax, VA 22033

Table of Contents

Section ***Page***

1. Executive Summary **1**

2. Background **3**

3. Detailed Finding

Configuration Management Controls for Operating System Software **7**

Appendix A: Objective, Scope, and Methodology **14**

Appendix B: Additional Information on the Capability Maturity Model Integration **16**

Appendix C: Laws and Regulations **18**

Appendix D: Acronyms **19**

Appendix E: Glossary of Terms **20**

List of Tables

Page

Table 1: Operating System Software Platforms Reviewed 5
Table 2: CMMI Bodies of Knowledge 16
Table 3: Capability Levels (Continuous Representation) Excerpts from the CMMI 17

List of Exhibits

Page

Exhibit 1: Software Configuration Management Principles of the CMMI 3
Exhibit 2: Change Management Process Steps 4
Exhibit 3: Configuration Identification 7
Exhibit 4: Configuration Control 8
Exhibit 5: Configuration Accounting 9
Exhibit 6: Configuration Auditing 9
Exhibit 7: Windows® Server and Desktop Software Configuration Changes 11

1. Executive Summary

The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) contracted with International Business Machines (IBM) Business Consulting Services (hereafter referred to as IBM) to audit and report on the effectiveness of the FDIC's configuration management controls over operating system software. Federal agencies are required by the Federal Information Security Management Act of 2002 (FISMA)[1] to establish and implement minimally acceptable configuration requirements for their information systems. In addition, agency Chief Information Officers (CIO) and Inspectors General are required by Office of Management and Budget (OMB) policy to assess and report on the implementation of agency configuration management controls as part of their annual FISMA reviews and evaluations. The results of this audit support the OIG in fulfilling its evaluation and reporting responsibilities under FISMA. IBM conducted its work in accordance with generally accepted government auditing standards.

The objective of the audit was to determine whether the FDIC had established and implemented configuration management controls over its operating system software that were consistent with federal standards and guidelines and industry-accepted practices. The scope of the audit focused on four of the FDIC's operating system software platforms: (1) Microsoft Windows® for servers, (2) Microsoft Windows® for desktop (and laptop) computers, (3) Sun Microsystems, Inc.'s Solaris™ for servers, and (4) Cisco IOS® for telecommunications. IBM chose these four platforms because they support many of the FDIC's sensitive and mission-critical business applications. IBM used the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems,* and the Capability Maturity Model Integration (CMMI)[2] developed by Carnegie Mellon University's Software Engineering Institute (SEI) as the primary criteria for conducting the audit. IBM chose the CMMI because it defines a generally accepted set of software configuration management principles, and the FDIC's Division of Information Technology (DIT) has embraced the CMMI as a means of achieving process improvement. The recommendations contained in this report are designed to promote compliance with federal standards and guidelines and further the FDIC's goal of achieving CMMI process improvements.

A detailed description of the audit's scope and methodology is contained in Appendix A. Appendix D contains a list of acronyms, and Appendix E contains a glossary of terms used in the report.

Results of the Audit

DIT established and implemented a number of configuration management controls over its operating system software that were consistent with federal standards and guidelines and industry-accepted practices. Such controls included a software patch management policy, a

[1] Appendix C contains additional information on the laws and regulations referenced in this report.

[2] CMMI Version 1.1 for *Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing* (Continuous Representation), dated March 2002. The CMMI is a process improvement methodology that defines six capability levels reflecting an organization's ability to perform, control, and improve its performance. Appendix B contains additional information on the CMMI. CMMI is a service mark of Carnegie Mellon University.

FDIC Infrastructure Change Control Board,[3] and periodic scanning of operating system software configurations. Such actions were positive; however, control improvements were needed. Specifically, DIT needed to establish an organizational policy and system-specific procedures to ensure proper configuration management of operating system software. DIT also needed to standardize and integrate the recording, tracking, and reporting of operating system software configuration changes to the extent practical. Collectively, these control weaknesses limited the FDIC's assurance that its configuration management practices were efficient and effective and that systems were configured to minimize the risk of security vulnerabilities and service interruptions. A summary of IBM's recommendations follows.

Summary Recommendations

IBM recommends that the FDIC CIO:

- Establish a policy that takes an enterprise approach to defining the roles, responsibilities, and overall principles and management expectations for performing configuration management on operating system software. The policy should address requirements for developing and maintaining configuration management plans and performing periodic self-assessments of configuration management processes and practices.
- Develop configuration management plan(s) covering the four operating system software platforms addressed in this report consistent with federal standards and guidelines and industry-accepted practices. DIT should determine whether other operating system software platforms require configuration management plan(s) and develop such plans where appropriate.
- Ensure that the certification and accreditation of the FDIC's general support systems incorporate an evaluation and testing of the FDIC's configuration management policy and plans referenced in recommendations 1 and 2 of this report.
- Document the minimum required configuration settings for the Windows® server and desktop operating system platforms, and develop procedures to ensure that changes to baseline configuration settings are documented.
- Standardize and integrate the recording, tracking, and reporting of operating system software configuration changes to the maximum extent practical. As part of this effort, DIT should consider using automated mechanisms to improve performance metric reporting for configuration changes from a system-specific and enterprise perspective.

[3] DIT established the FDIC Infrastructure Change Control Board in February 2005 to formally review and approve changes to the information technology infrastructure and technical architecture; ensure that changes are well planned, communicated, and coordinated; and manage the change control process.

2. Background

Key to ensuring the integrity, security, and reliability 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. Typical changes that should be subject to formal configuration management in the operating system software environment include the installation of security patches that address known vulnerabilities, programs that support system maintenance, and upgrades (referred to as "service packs") that improve system performance, security, and functionality. Without disciplined processes for controlling software changes, management cannot be assured that its systems will operate as intended, that software defects will be minimized, or that systems maintenance will be performed in a cost-effective or timely manner.

A number of internationally recognized software configuration management standards are in wide use today. These include standards published by the SEI,[4] Project Management Institute, American National Standards Institute/Institute of Electrical and Electronic Engineers, and International Organization for Standardization. IBM selected SEI's CMMI as a key criterion for conducting the audit because the CMMI defines generally accepted software configuration management principles, and DIT has embraced the CMMI as a means of achieving information technology (IT) process improvement. In addition, the configuration management principles embodied in the CMMI are consistent with the configuration management security controls defined in NIST SP 800-53 for non-national security federal information systems. Exhibit 1 depicts the software configuration management principles of the CMMI. These four principles are based on the best practices of carefully chosen disciplines, including systems analysis and design and software engineering. IBM's audit results are organized around these four fundamental principles, which are described in greater detail below.

Exhibit 1: Software Configuration Management Principles of the CMMI

Source: IBM Analysis of the CMMI.

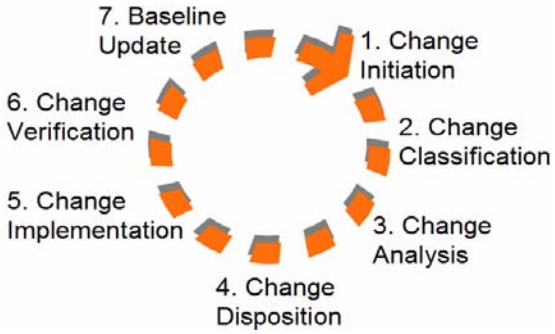
Configuration Identification involves the establishment of baseline configurations for "work products" that are subject to configuration management. Typical work products subject to configuration management within the operating system environment include software, such as the system itself and its component parts, and documents, such as server and desktop build procedures, systems inventories, and configuration management plans. Establishing and enforcing baseline configurations is critical to reducing software maintenance costs and ensuring secure and reliable systems. For example, without a baseline configuration for desktop operating systems, such as Microsoft Windows® XP Professional Service Pack 2, organizations would

[4] SEI is a federally funded software engineering research and development center sponsored by the Department of Defense. Founded in 1984, SEI's mission is to assist organizations in improving their software engineering capabilities.

expend excessive time and resources patching, troubleshooting, and testing changes for earlier desktop versions of Windows®, such as Windows® XP Professional Service Pack 1. Baseline configurations serve as the basis for future development and should be modified only through the change control processes described under *Configuration Control* below.

Configuration Control is the heart of configuration management because it involves implementing a change management system to systematically control and monitor changes to the baseline configurations established under *Configuration Identification*. A change management system consists of policies, procedures, automated tools, and other controls for performing the change management process steps depicted in Exhibit 2. *Configuration Control* ensures that proposed software changes are properly evaluated for compliance with applicable standards, assessed and tested to avoid potential disruptions or compromise of system security, approved or disapproved by appropriate authorities, verified upon completion, and reflected in baseline configurations.

Exhibit 2: Change Management Process Steps



Source: IBM Analysis of the CMMI.

Configuration Status Accounting is the recording and reporting of configuration management activities in sufficient detail to provide stakeholders with information needed to manage their work products. Such information can include metrics such as the number of in-process and completed configuration changes at a particular point in time, the average time spent processing high-priority or low-priority changes, and the number of changes that address new requirements or defects in work products.[5] By performing trend analysis of such metrics, management can identify potential problems in its configuration management processes. *Configuration Status Accounting* information is used to make important policy, resource, and budget decisions and assists managers in determining whether configuration management processes and practices are efficient, effective, and achieving intended results. Due to the complexity and volume of configuration changes associated with operating system software, many organizations use automated configuration management tools to centrally track, record, and report the status of configuration changes.

Configuration Auditing involves the self-assessment of an organization's configuration management activities and processes to determine whether controls function as intended. Such self-assessments provide management with assurance that baseline configurations and related documentation are current, accurate, and complete and that implemented changes can be traced

[5] Examples of configuration changes resulting from defects in work products include (1) the redeployment of a software patch because the original deployment did not successfully install on all target servers or workstations or (2) corrective actions to address a software functionality problem caused by incompatibility. Tracking such changes is important because they could be an indication of inadequate testing or other configuration management problems.

to original requirements. The results of configuration management audits can be subject to review by independent third parties.

Roles and Responsibilities for Operating System Software

DIT has overall responsibility for maintaining the configuration of the FDIC's operating system software. Responsibility for maintaining the configuration of individual operating system software platforms is shared among two branches and several sections within DIT's Infrastructure Services (IS). Table 1 below identifies the four operating system software platforms selected for the audit, along with a brief description of the platform and the IS section with primary responsibility for its configuration.

Table 1: Operating System Software Platforms Reviewed

Operating System Software Platform	General Description	IS Branch/Section With Primary Responsibility
Microsoft Windows® for Servers	Windows® 2000 Advance Server is the standard operating system in the network server environment.* The Windows® server platform supports network-based applications, such as the New Financial Environment and FDICconnect, as well as IT services for managing the network.	Software Support Branch, Server Software Section Operations Branch, LAN Management Section
Microsoft Windows® for Desktop (and Laptop) Computers	Windows® XP Professional is the standard operating system in the desktop computer environment. Windows® XP Professional primarily supports user productivity tools, such as the Internet Explorer and Microsoft Office Suite.	Software Support Branch, Client Software Section Operations Branch, LAN Management Section
Sun Microsystems, Inc., Solaris™	Solaris™ is the standard operating system in the UNIX® environment. Solaris™ supports core IT infrastructure services, such as the Public Key Infrastructure, and a number of business applications, such as the Overarching Automation System and Corporate Human Resources Information System Time and Attendance system.	Software Support Branch, Server Software Section Operations Branch, Telecommunications Section
Cisco IOS®	Cisco IOS® supports the routing, message processing, and protocol interfaces needed to transfer data over the FDIC's LANs, metropolitan area networks, and wide area network.	Operations Branch, Telecommunications Section

* At the time of our audit, DIT supported a limited number of servers operating the Windows NT® and Windows® 2003 operating systems.

Recent Control Improvements

DIT has taken a number of recent actions to strengthen its configuration management controls over operating system software, and additional improvements were underway during the audit. Of particular note, DIT issued a formal patch management policy,[6] established the FDIC Infrastructure Change Control Board, and strengthened its security vulnerability scanning techniques[7] for network devices. DIT also established a new performance-based contracting structure in September 2004 that included a service-level agreement to achieve CMMI process improvement in infrastructure operations (including software configuration management). In addition, DIT was working to improve the integrity of patch information reported by the Microsoft Systems Management Server (SMS) 2003[8] and implement Symantec's Enterprise Security Manager on the FDIC's IT infrastructure to better monitor the configuration of Windows® servers. While such improvements promote an enterprise-wide approach to performing configuration management, additional controls are needed to ensure proper management of operating system software configuration.

[6] DIT Policy Memorandum 04-004, *Policy on Security Patch Management*, dated April 15, 2004.

[7] DIT began using the Harris Corporation's Security Threat Avoidance Technology (STAT®) vulnerability assessment scanner in December 2004.

[8] SMS is a key configuration management tool used on the Windows® server and desktop computing platforms. DIT uses SMS to remotely scan devices on these software platforms, inventory installed software, distribute security patches and other software, and generate reports on installed/uninstalled software.

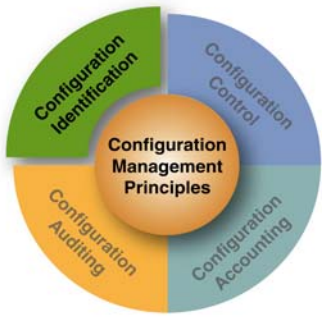
3. Detailed Finding: Configuration Management Controls for Operating System Software

CONDITION

DIT established and implemented a number of configuration management controls over its operating system software that were consistent with federal standards and guidelines and industry-accepted practices. Such controls included a software patch management policy, an FDIC Infrastructure Change Control Board, and periodic scanning of operating system software configurations. Such actions were positive; however, control weaknesses existed relating to each of the four configuration management principles defined in the CMMI. A description of these weaknesses follows.

Configuration Identification

Exhibit 3: Configuration Identification



Source: IBM Analysis of the CMMI.

DIT used a number of key work products, such as server and desktop build procedures, ghost imaging procedures, software image files, and system inventories, to manage the configuration of the four operating system software platforms that we reviewed. DIT had not subjected these work products to formal configuration management, as defined by the CMMI, to ensure that they were current, accurate, and complete. Specifically, DIT had not developed procedures for (1) identifying work products that should be subject to configuration management, (2) designating responsibility for maintaining current and historical versions of work products, (3) designating authority to approve changes to work products, and (4) determining when work products should be revised.[9] Such procedures are typically documented in a configuration management policy and/or system configuration management plan(s).

DIT defined configuration procedures in various documents but had not documented procedures for the ongoing identification and documentation of minimum custom baseline configuration settings applicable to the Windows® server and desktop operating system platforms. Custom configuration settings include, for example, registry permissions, Internet Explorer settings, local system security settings, and unnecessary computer services that should be disabled or uninstalled. In OIG Audit Report No. 05-016 entitled, *Audit of Security Controls Over the FDIC's Electronic Mail Infrastructure*, dated March 31, 2005, IBM noted that DIT had not documented procedures for disabling unnecessary computer services on Exchange e-mail servers when appropriate. Based on a sample of 15 e-mail servers, IBM identified 6 computer services that had been enabled but were not required for processing e-mail. The six unnecessary computer services presented a potential security risk because they could have been exploited by a virus, worm, or other malicious program to damage the FDIC's IT resources.

[9] Organizations can use different criteria for determining when a work product subject to configuration management should be revised. For example, an organization may require that its desktop build procedures and associated software image files be updated only following a major operating system upgrade, while another organization may require updates to these same work products periodically, such as monthly.

Configuration Control

Exhibit 4: Configuration Control

Source: IBM Analysis of the CMMI.

DIT had not standardized or integrated its processes for tracking and recording configuration changes within or across its operating system software platforms to ensure that such changes were properly controlled, accounted for, and reported. For example, software-related changes[10] for one of four operating system software platforms reviewed (i.e., Windows® server) were documented using standard forms that were stored in a central location. However, hardware-related changes[11] for this same platform were neither recorded using a standard form nor stored in a central repository. In order to obtain information about hardware-related changes for this platform, such as when a change was made, who implemented a change, testing that was performed for a change, or who verified a change, IBM had to speak with systems personnel with first-hand knowledge of the changes. Configuration changes for another of the four operating system software platforms (i.e., Sun Microsystems, Inc.'s Solaris™ for servers) were either managed through an automated change management tool[12] or recorded in various Microsoft Word documents, depending on which IS branch and section had responsibility for the servers affected by the change.

Although DIT had developed test plans and roll-back plans[13] for its major operating system upgrades, test plans and roll-back plans were generally not documented for other configuration changes. Although IS personnel stated that they had tested configuration changes before they were implemented, test plans and test results were not documented for 22 of 25 judgmentally selected configuration changes to the four operating system software platforms. In addition, 21 of 25 configuration changes did not have a documented roll-back plan. Test plans, roll-back plans, and test results are important for ensuring that configuration changes function as intended and have no negative impact on IT operations. In January 2005, several hundred FDIC users were unable to access their Outlook e-mail for several days following an unsuccessful configuration change to a key e-mail server. IBM noted that DIT had not documented a test plan, test results, or roll-back plan for this configuration change. Test results also document system incompatibilities and management's rationale for making specific configuration decisions. The level of documentation needed for test plans, roll-back plans, and test results should be based on the risk and complexity of a configuration change and could be as simple as a completed checklist or memorandum.

---

[10] Software-related changes include, for example, the installation or removal of items such as service packs, security patches, and software programs.

[11] Hardware-related changes include, for example, the installation or removal of items such as network interface cards and server hard drives. Hardware-related changes can directly impact the performance of operating system software.

[12] The tool used was the FDIC Change Management System (FCMS). FCMS has formal automated workflow process capabilities, such as the ability to track, record, and report configuration change requests.

[13] Sometimes referred to as a "back-out plan," a roll-back plan describes the system recovery steps to be followed should a configuration change cause an unexpected, negative effect on an organization's IT operations.

Configuration Accounting

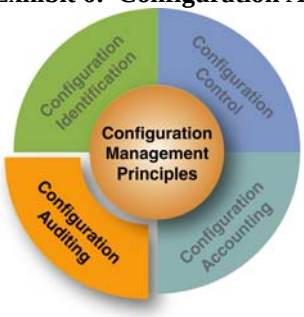
Exhibit 5: Configuration Accounting

Source: IBM Analysis of the CMMI.

DIT collected and reported configuration status information on the four operating system software platforms that we reviewed through a variety of means, including the FDIC Infrastructure Change Control Board meetings, SMS reports on patch deployments, and software scanning techniques. However, DIT did not track or report key configuration management metrics within or across its operating system software platforms. Such metrics could include, for example, the number of in-process and completed configuration changes, the status of in-process changes, or the average amount of time (i.e., speed) to implement high-priority versus low-priority changes. In addition, because DIT did not classify configuration changes as addressing new requirements or defects in work products, DIT was unable to determine the amount of effort expended to enhance software versus correct problems.

Configuration Auditing

Exhibit 6: Configuration Auditing



Source: IBM Analysis of the CMMI.

DIT used various automated tools to evaluate the configuration of its operating system software,[14] but had not developed self-assessment procedures for determining whether configuration management controls functioned as intended. Developing self-assessment procedures is a recognized practice in configuration management and could be used to detect or prevent the types of process weaknesses identified in this report. Common self-assessment procedures include evaluating the integrity of key work products subject to configuration management; determining whether change request documentation is current, accurate, and complete; inspecting configuration changes for compliance with applicable policies, procedures, and guidelines; and verifying that configuration changes have been implemented as intended.

CAUSE

Several causes contributed to the control weaknesses in DIT's configuration management processes and practices as discussed below.

Organizational Policy and System-Specific Procedures

Circular 1320.4, *FDIC Software Configuration Management Policy*, dated July 8, 2003, establishes key roles and responsibilities, management expectations, and requirements for configuration management (including the need for configuration management plans, reviews of configuration management processes, and the use of automated configuration management tools). However, the circular is limited to application software and does not address operating

[14] Such tools included SMS, the Foundstone vulnerability scanner, the Harris Corporation's STAT scanner, and the Shavlik patch scanner.

system software. An organizational configuration management policy should define overall principles and expectations for performing operating system software configuration management and the associated roles and responsibilities of key personnel and organizational components, such as system engineers, administrators, and the FDIC Infrastructure Change Control Board. The policy should also address, and be a critical component of, the certification and accreditation process for operating system software.[15] An organizational policy is an important component of an enterprise approach to software configuration management.

DIT documented a number of its configuration management practices in various policies and procedures and established the FDIC Infrastructure Change Control Board to oversee configuration changes to the FDIC's operating system software. However, DIT had not developed configuration management plan(s) for any of the four operating system software platforms that IBM audited. Configuration management plans are a fundamental control for maintaining proper configuration of information systems because the plans define procedures for evaluating, classifying, authorizing, testing, documenting, and verifying configuration changes. These plans also define the system-specific roles and responsibilities (including controls for ensuring appropriate separation of duties) of key stakeholders and procedures for identifying, maintaining, and updating work products subject to configuration management. In addition, configuration management plans can describe the type and frequency of configuration status information to be tracked and reported to management, training requirements for key personnel, and requirements for conducting self-assessments of configuration management controls. Configuration management plans are an important component of system certification and accreditation. Because systems vary in complexity and design, configuration management plans should be tailored to the requirements of individual systems.

Automated Workflow Processes

The lack of standardization and integration in DIT's practices of recording, tracking, and reporting system configuration changes was caused primarily by a lack of automated workflow processes using configuration management tools. System change requests for three of four operating system software platforms reviewed were not managed with an automated workflow process tool. Although DIT used a workflow process tool to manage change requests on the remaining platform (i.e., Sun Microsystems, Inc.'s Solaris™ for servers), the tool was not used to track all change requests on the platform. In addition, system change requests for two other platforms (i.e., Windows® server and desktop) were generally stored in Outlook e-mail folders and Microsoft Word documents rather than in a central repository that could be used for tracking, reporting, or interfacing with other corporate systems, such as REMEDY®.[16] The lack of automated workflow processes using configuration management tools contributed to the absence of meaningful configuration management metrics discussed earlier.

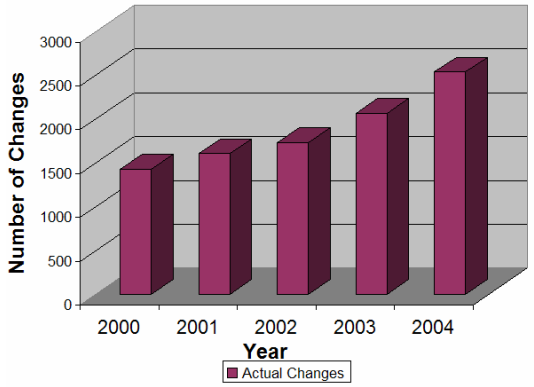
---

[15] Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

[16] REMEDY is used to track trouble tickets and IT hardware inventory.

Exhibit 7 illustrates the combined number of application and infrastructure configuration changes affecting two of the four operating system software platforms that IBM reviewed.[17] An automated workflow process tool to manage such a large number of configuration changes offers many advantages, such as defined business processes built into the tool that promote consistent, auditable, and repeatable change control practices. Configuration requirements can vary from system to system. Therefore, a single automated workflow process tool may not satisfy all configuration management needs. Selecting a workflow process tool should be based on an assessment of DIT's existing information systems and commercially available software products.

Exhibit 7: Windows® Server and Desktop Software Configuration Changes



Source: Analysis of DIT's Windows® Implementation Announcements Outlook E-Mail Folders.

CRITERIA

The CMMI, NIST, and OMB have established a number of guiding principles for effective software configuration management as discussed below.

Organizational Policy and System-Specific Procedures

The CMMI identifies an organizational configuration management policy as an important control for effectively planning and performing software configuration management. According to the CMMI, the configuration management policy defines organizational expectations for establishing and maintaining configuration baselines and tracking and controlling changes to work products subject to configuration management. Additionally, NIST SP 800-53 references a "formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance [i.e., self-assessments]" as a recommended security control for protecting federal information systems.

A key practice in the CMMI is performing periodic audits (i.e., self-assessments) of configuration management activities and processes to ensure the integrity of baseline configurations and related documentation. Self-assessments evaluate compliance with applicable configuration management standards and procedures and verify the integrity of items in the configuration management system based on requirements documented in the configuration management plan. In addition, NIST SP 800-53 recognizes audit activities associated with configuration changes to federal information systems as a recommended security practice.

The CMMI recognizes the importance of establishing and maintaining a configuration management plan. According to the CMMI, an important configuration management practice is

[17] IBM was unable to determine the number of configuration changes relating to the infrastructure because infrastructure changes were not stored separately from application changes.

identifying work products that will be subject to configuration management based on documented criteria and designating individuals responsible for work product maintenance. NIST SP 800-53 identifies a configuration management plan as a recommended security control for protecting federal information systems. The NIST publication also references "formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls" as a component of a security control structure. In addition, NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, notes that configuration management plans are a key security-related document that can be part of the security accreditation package. The Computer Security Division of NIST maintains examples of configuration management plans for operating system software at its Web site http://csrc.nist.gov/fasp under the link entitled "*FASP Areas*."[18]

Further, NIST SP 800-53 recognizes the importance of maintaining an organization-defined list of prohibited computer services and configuring IT products to the most restrictive mode consistent with system operational requirements. In addition, NIST SP 800-70, *The NIST Security Configuration Checklists Program*, contains detailed guidance that should be used when configuring operating system software settings.

Automated Workflow Processes

The CMMI addresses the importance of establishing and maintaining a change management system to store, update, and retrieve configuration management records and other work products subject to configuration management. The change management system includes a change request database wherein change requests are initiated and recorded and configuration management reports are generated. NIST SP 800-53 states that organizations should employ automated mechanisms to (i) document proposed changes to the system, (ii) notify appropriate approval authorities, (iii) identify approvals that have not been received in a timely manner, (iv) inhibit change until necessary approvals are received, and (v) document completed changes to the information system. NIST SP 800-53 also recognizes that organizations should employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration. Automating change control practices is also consistent with DIT's infrastructure services contract, which requires contractor personnel, whenever possible and practical, to consolidate IT platforms and operations, integrate infrastructure requirements into efficient and effective solutions, and capture and deliver information in real or near-real time using electronic means.

OMB Circular No. A-130, *Management of Federal Information Resources*, dated November 28, 2000, requires agencies to institute performance measures and management processes that monitor actual performance against expected results. The CMMI describes various types of configuration metrics, such as the status of change requests and number of change requests related to software defects, that are part of configuration management. Such metrics would be a valuable asset to DIT management in evaluating the performance of the FDIC's IT infrastructure services contractors.

[18] Federal Agency Security Practices (FASP). The FASP effort was initiated as a result of the success of the Federal CIO Council's Federal Best Security Practices pilot effort to identify, evaluate, and disseminate best practices for critical infrastructure protection and security.

EFFECT

The lack of an organizational policy and system-specific configuration management procedures limited the FDIC's assurance that its information systems were configured to minimize the risk of security vulnerabilities and IT service interruptions. Absent appropriate policies and procedures, DIT is overly dependent on the knowledge and experience of individual system engineers and administrators to maintain minimum baseline configuration settings consistently across platforms. The lack of automated workflow processes impaired DIT's ability to efficiently and effectively manage system configuration changes throughout the systems' life cycle and to report meaningful configuration metrics to management. In addition, the lack of periodic self-assessments of configuration management controls limited DIT's assurance that key work products were current, accurate, and complete and that configuration management processes were efficient, effective, and achieving intended results.

RECOMMENDATIONS

IBM recommends that the FDIC CIO:

1. Establish a policy that takes an enterprise approach to defining the roles, responsibilities, and overall principles and management expectations for performing configuration management on operating system software. The policy should address requirements for developing and maintaining configuration management plans and performing periodic self-assessments of configuration management processes and practices.

2. Develop configuration management plan(s) covering the four operating system software platforms addressed in this report consistent with federal standards and guidelines and industry-accepted practices. DIT should determine whether other operating system software platforms require configuration management plan(s) and develop such plans where appropriate.

3. Ensure that the certification and accreditation of the FDIC's general support systems incorporate an evaluation and testing of the FDIC's configuration management policy and plans referenced in recommendations 1 and 2 of this report.

4. Document the minimum required configuration settings for the Windows® server and desktop operating system platforms and develop procedures to ensure that changes to baseline configuration settings are captured and documented.

5. Standardize and integrate the recording, tracking, and reporting of operating system software configuration changes to the maximum extent practical. As part of this effort, DIT should consider using automated mechanisms to improve performance metric reporting for configuration changes from a system-specific and enterprise perspective.

APPENDIX A: OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of the audit was to determine whether the FDIC had established and implemented configuration management controls over its operating system software that were consistent with federal standards and guidelines and industry-accepted practices. The scope of the audit focused on four operating system software platforms: (1) Microsoft Windows® for servers,[19] (2) Microsoft Windows® for desktop (and laptop) computers, (3) Sun Microsystems, Inc.'s Solaris™ for servers, and (4) Cisco IOS® for telecommunications. IBM chose these four platforms because they support many of the FDIC's sensitive and mission-critical business applications. The audit did not include an evaluation of the FDIC's configuration management controls over applications running on the four operating system software platforms because DIT was performing an internal assessment of application configuration management controls.

To accomplish the audit objective, IBM interviewed key DIT personnel who had responsibility for maintaining the configuration of the four operating system software platforms. IBM reviewed relevant FDIC policies, procedures, and guidelines and evaluated key documents and reports, such as server and desktop build procedures, system security plans, and DIT's *Daily Reports for Technical Infrastructure*. IBM also reviewed DIT's security self-assessment procedures that were designed to ensure the secure configuration of the four selected platforms. In addition, IBM evaluated DIT's change control procedures for each of the four platforms by testing a judgmental sample of configuration changes. Using source documentation and DIT's automated systems of record, IBM determined whether selected configuration changes had been properly authorized, evaluated, tested, tracked, implemented, and reported. IBM coordinated its work with an ongoing DIT internal assessment of the security patch management process for desktop computers.

IBM used NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, and the configuration management principles defined in the CMMI, developed by Carnegie Mellon University's SEI, as the primary criteria for conducting the audit. In addition, IBM used relevant provisions of the Government Accountability Office's *Federal Information System Controls Audit Manual*[20] and NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, as supplemental criteria. The OIG evaluated the nature, timing, and extent of work described in IBM's audit program, obtained an understanding of IBM's methodologies and assumptions, attended key meetings, monitored progress throughout the audit, and performed other appropriate procedures. In this manner, the OIG was able to assure itself that, except for the performance of an external peer review, IBM's audit work complied with generally accepted government auditing standards. IBM conducted its field work from October 2004 through June 2005.

[19] The FDIC's standard server-based operating system in the network environment is Microsoft Windows® 2000 Advance Server. At the time of our audit, DIT was maintaining a limited number of servers operating the Windows NT® and Windows® 2003 operating systems.

[20] The manual provides guidance for reviewing information system controls (including software configuration management controls) that affect the integrity, confidentiality, and availability of computerized data.

Prior Audit Coverage

On September 1, 2000, the OIG issued Audit Report No. 00-038 entitled, *Audit of the Information Technology Configuration Management Program*. The report states that the then Division of Information Resources Management (now DIT) was in the process of developing a plan to establish a formal IT configuration management program. The report discusses the salient components of effective configuration management and recommends considering these components in developing and implementing a formal configuration management program. FDIC management had taken action sufficient to close the recommendation.

Computer-based Data, Performance Measures, and Illegal Acts

IBM performed appropriate procedures to ensure that computer-based data were valid and reliable when those data were significant to the audit's findings and conclusions. Such procedures included verifying selected automated data to source documentation and corroborating automated data through interviews with appropriate DIT personnel. In addition, IBM evaluated whether DIT's configuration management performance metrics for operating system software were consistent with federal and industry guidance. Finally, IBM did not develop specific audit procedures to detect fraud and illegal acts because they were not considered material to the audit objective. However, throughout the audit, IBM was sensitive to the potential of fraud, waste, abuse, and mismanagement.

APPENDIX B: ADDITIONAL INFORMATION ON THE CAPABILITY MATURITY MODEL INTEGRATION

The CMMI combines a carefully chosen set of best practices based on experience in four bodies of knowledge (described in Table 2 below). Organizations from industry, government, and Carnegie Mellon University's SEI jointly developed the CMMI to provide organizations a mechanism to effectively appraise their process area capabilities, establish priorities, and implement improvements.

Table 2: CMMI Bodies of Knowledge

Body of Knowledge	Description
System Engineering	Covers the development of total systems, which may or may not include software. Systems engineers focus on transforming customers' needs, expectations, and constraints into products and supporting these products throughout their life cycle.
Software Engineering	Covers the development of software systems. Software engineers focus on applying systematic, disciplined, and quantifiable approaches to the development, operation, and maintenance of software.
Integrated Product and Process Development	Provides a systematic approach that achieves a timely collaboration of relevant stakeholders throughout the life of a product to satisfy customers' needs, expectations, and requirements. The processes to support an Integrated Product and Process Development approach are integrated with the other processes in the organization.
Supplier Sourcing	Covers the use of suppliers to perform functions or add modifications to products that are specifically needed by a project. Projects benefit from enhanced source analysis and monitoring supplier activities before product delivery.

The CMMI supports two representations: *staged* and *continuous*. The *staged representation* provides a proven sequence of improvements, beginning with basic management practices and progressing through a pre-defined and proven path of successive levels, each serving as a foundation for the next. The *staged representation* permits comparisons across and among organizations by the use of overall, organization-wide maturity levels. The *continuous representation* allows an organization to select the order of improvement that best meets its business objectives and mitigates the organization's areas of risk. The *continuous representation* enables comparisons across and among organizations on a process-area-by-process-area basis, using the six capability levels depicted in Table 3 on the next page. Both representations are designed to achieve essentially equivalent results.

Table 3: Capability Levels (Continuous Representation)
Excerpts From the CMMI

Capability Level	Capability Level Description
0	**Incomplete.** Reflects processes that are either not performed or partially performed.
1	**Performed.** Reflects processes that support and enable the work needed to produce identified work products.
2	**Managed.** Reflects processes that are planned and executed in accordance with policy, employ skilled people having adequate resources to produce controlled outputs, involve relevant stakeholders, are monitored, controlled, and reviewed, and are evaluated for adherence to its process description. A critical distinction between a performed process and a managed process is the extent to which the process is managed. A managed process is planned, and the performance of the process is managed against the plan. Corrective actions are taken when the actual results and performance deviate significantly from the plan.
3	**Defined.** Reflects managed processes that are tailored from the organization's set of standard processes according to the organization's tailoring guidelines and contributes work products, measures, and other process-improvement information to the organizational process assets. The organization's set of standard processes, which are the basis of the defined process, are established and improved over time.
4	**Quantitatively Managed.** Reflects processes that are controlled using statistical and other quantitative techniques. Quantitative objectives for quality and process performance are established and used as criteria in managing the process.
5	**Optimizing.** Reflects processes that are quantitatively managed and changed and adapted to meet relevant current and projected business objectives. An optimizing process focuses on continually improving process performance through both incremental and innovative technological improvements. Process improvements that would address root causes of process variation and measurably improve the organization's processes are identified, evaluated, and deployed as appropriate.

IBM used the *CMMI Version 1.1 for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing (Continuous Representation),* dated March 2002, (CMMI-SE/SW/IPPD/SS, V1.1) as a key criterion for conducting the audit because the CMMI defines generally accepted software configuration management principles, and DIT has embraced the CMMI as a means of achieving IT process improvement.

APPENDIX C: LAWS AND REGULATIONS

Below are the key statutes, regulations, standards, and guidelines that were considered during the audit. Statutory and regulatory sources may not be legally binding on the FDIC; see individual references for further information.

Federal Information Security Management Act (FISMA), title III, *E-Government Act of 2002*, Pub. L. No. 107-347, dated December 17, 2002
http://www.cio.gov/archive/e_gov_act_2002.pdf

Enacted as part of the E-Government Act of 2002, FISMA permanently re-authorized and strengthened the information security program, evaluation, and reporting requirements established by the Government Information Security Reform Act (GISRA), which expired in November 2002. FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources supporting federal operations and assets. Among its provisions, FISMA requires federal agencies to establish and implement minimally acceptable configuration requirements for their information systems; see section 301(b). For purposes of that section, the FDIC is considered an agency and is, therefore, subject to its provisions.

OMB Circular No. A-130, *Management of Federal Information Resources* (Transmittal Memorandum No. 4) Appendix III, *Security of Federal Automated Information Resources*, dated November 2000 (OMB A-130, Appendix III)
http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

OMB A-130, Appendix III, establishes minimum controls for federal automated information security programs. The FDIC's Legal Division has opined that portions of the circular apply to the FDIC, while other portions do not apply. The Legal Division specifically opined that Appendix III of the circular legally requires the FDIC to implement and maintain an information security program consistent with government-wide policies, standards, and procedures issued by the OMB and the U.S. Department of Commerce.

NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, dated February 2005
http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf

The publication defines minimum recommended security controls for non-national security federal information systems based on the impact levels defined in NIST Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. NIST SP 800-53 provides guidelines for selecting and specifying minimum security controls for federal information systems until the publication of FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* (projected for publication December 2005). The guidelines have been developed to help achieve more secure systems within the federal government. NIST SPs are, by their own terms, guidelines (rather than mandatory requirements) for agencies in implementing their IT operations.

APPENDIX D: ACRONYMS

Acronyms	Definition
CIO	Chief Information Officer
CMMI	Capability Maturity Model Integration
DIT	Division of Information Technology
FCMS	FDIC Change Management System
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Management Act
IBM	International Business Machines Business Consulting Services
IS	Infrastructure Services
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action & Milestones
SEI	Software Engineering Institute
SMS	Systems Management Server
SP	Special Publication

APPENDIX E: GLOSSARY OF TERMS

Term	Definition
Accreditation	Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.
Baseline	A set of configuration items that has been reviewed and agreed upon and, thereafter, serves as the basis for future management, development, or maintenance.
Build Procedures	Automated and documented procedures used for installing operating system software on servers and desktops.
Capability Level	A capability level consists of related specific and generic practices for a process area that can improve the organization's processes associated with that process area.
Certification	Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Configuration Accounting	An element of configuration management consisting of the recording and reporting of information needed to manage a configuration effectively.
Configuration Audit	A self-assessment conducted to verify that a configuration item conforms to a specified standard or requirement.
Configuration Control	An element of configuration management consisting of the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items following configuration identification.
Configuration Identification	An element of configuration management consisting of selecting configuration items for a product, assigning unique identifiers to them, and recording their functional and physical characteristics in technical documentation.
Configuration Item	An aggregation of work products designated for configuration management and treated as a single entity in the configuration management process.

Term	Definition
General Support System	An interconnected set of information resources under the same direct management control. This system normally includes hardware, software, information, data, applications, communications, and people.
National Institute of Standards and Technology	A non-regulatory federal agency within the U.S. Department of Commerce's Technology Administration. NIST 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.
Plan of Action and Milestones	A plan of action and milestones (POA&M), sometimes referred to as a corrective action plan, is a tool that identifies tasks to be accomplished. It details resources required to accomplish the elements of the plan, milestones in meeting the task, and scheduled completion dates for the milestones. POA&Ms assist management in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for weaknesses identified in programs and systems.
Roll-back Plan	A documented plan (sometimes called a "back-out plan") that describes the system recovery steps to be followed should a configuration change cause an unexpected, negative effect on an organization's IT operations.
Security Vulnerability	A flaw or weakness in the design or implementation of an information system (including the security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely affect an organization's operations or assets through a loss of confidentiality, integrity, or availability.
Software Configuration Management	The technical and administrative processes of identifying, documenting, and maintaining configuration item integrity; controlling configuration item changes; recording and reporting on configuration item change status; and verifying compliance with policy.
Work Product	An artifact produced by a process, such as server and desktop build procedures, ghost imaging procedures, software image files, system inventories, and other files, documents, services, processes, and specifications.

Part II

Corporation Comments and OIG Evaluation

CORPORATION COMMENTS AND OIG EVALUATION

The report contains five recommendations directed to the CIO. The CIO's response to the draft report is presented in its entirety, beginning on page II-6. DIT concurred with two of the report's recommendations, and partially concurred with the remaining three recommendations. Based on the CIO's response, the five report recommendations are considered resolved but will remain undispositioned and open until we have determined that agreed-to corrective actions have been completed and are effective. The CIO's responses for each of the report's recommendations are summarized below along with our evaluation of the responses.

Recommendation 1: The CIO should establish a policy that takes an enterprise approach to defining the roles, responsibilities, and overall principles and management expectations for performing configuration management on operating system software. The policy should address requirements for developing and maintaining configuration management plans and performing periodic self-assessments of configuration management processes and practices.

DIT Response: DIT partially concurs with the recommendation. DIT does not believe that a single policy covering all types of software is necessarily the best approach. However, DIT agrees to review its policies to determine how to effectively cover configuration management of the various operating systems and will develop appropriate modifications to existing policies or a new policy, as required, to meet the intent of the recommendation. The new and/or revised policy will be established from a high-level, enterprise approach that will address requirements for configuration management plans and periodic self-assessments.

OIG Evaluation of Response: DIT's response meets the intent of our recommendation. The recommendation is resolved but will remain undispositioned and open until we have determined that agreed-to corrective action has been completed and is effective.

Recommendation 2: The CIO should develop configuration management plan(s) covering the four operating system software platforms addressed in this report consistent with federal standards and guidelines and industry-accepted practices. DIT should determine whether other operating system software platforms require configuration management plan(s) and develop such plans where appropriate.

DIT Response: DIT concurs with the recommendation. DIT will incorporate current server configuration procedures and practices into configuration management plans consistent with federal standards and guidelines for the four operating systems covered by the audit. DIT will also determine whether other operating system software platforms require configuration management plan(s) and develop such plans as appropriate.

OIG Evaluation of Response: The recommendation is resolved but will remain undispositioned and open until we have determined that agreed-to corrective action has been completed and is effective.

Recommendation 3: The CIO should ensure that the certification and accreditation of the FDIC's general support systems incorporate an evaluation and testing of the FDIC's configuration management policy and plans referenced in recommendations 1 and 2 of this report.

DIT Response: DIT partially concurs with the recommendation. DIT stated that the FDIC's security test and evaluation (ST&E) process, a component of the certification and accreditation (C&A) program, evaluates configuration management policies, procedures, and plans for compliance with NIST guidance and industry best practices. Once the new configuration management policy and plans are developed, DIT agrees to include evaluation and testing of the policy and plans in future C&A cycles.

OIG Evaluation of Response: DIT's response meets the intent of the recommendation. The recommendation is resolved but will remain undispositioned and open until we have determined that agreed-to corrective action has been completed and is effective.

Recommendation 4: The CIO should document the minimum required configuration settings for the Windows® server and desktop operating system platforms and develop procedures to ensure that changes to baseline configuration settings are documented.

DIT Response: DIT partially concurs with the recommendation. DIT indicated that it has several processes to document required configuration settings for Windows® servers and desktop operating systems, including server build procedures. However, DIT agrees to review its current procedures to ensure that standard baseline configurations and approved exceptions to configuration settings are fully documented. DIT will also re-emphasize compliance with operational procedures established to ensure that server and desktop build procedures are consistently applied for each operating system. Additionally, DIT will evaluate the feasibility of adopting automated tool(s) that can facilitate periodic review of configuration settings to monitor compliance with build standards.

OIG Evaluation of Response: DIT's response meets the intent of the recommendation. The recommendation is resolved but will remain undispositioned and open until we have determined that agreed-to corrective action has been completed and is effective.

Recommendation 5: The CIO should standardize and integrate the recording, tracking, and reporting of operating system software configuration changes to the maximum extent practical. As part of this effort, DIT should consider using automated mechanisms to improve performance metric reporting for configuration changes from a system-specific and enterprise perspective.

DIT Response: DIT concurs with the recommendation. DIT stated that it has been working to standardize a single system for tracking and documenting configuration changes and improving performance metric reporting.

OIG Evaluation of Response: The recommendation is resolved but will remain undispositioned and open until we have determined that agreed-to corrective action has been completed and is effective.

MANAGEMENT RESPONSE TO RECOMMENDATIONS

This table presents the management response on the recommendations in our report and the status of the recommendations as of the date of report issuance.

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Dispositioned:[b] Yes or No	Open or Closed[c]
1	DIT will modify existing policies or develop a new policy that addresses configuration management principles from a high-level, enterprise approach and that addresses requirements for configuration management plans and periodic self-assessments.	November 30, 2005	N/A	Yes	No	Open
2	DIT will incorporate operating system software configuration management procedures and practices into configuration management plans consistent with federal standards and guidelines.	March 15, 2006	N/A	Yes	No	Open
3	DIT will include new configuration management policies and plans in future certification and accreditation cycles.	June 30, 2006	N/A	Yes	No	Open
4	DIT will (1) review its current procedures to ensure that standard baseline configurations and approved exceptions to configuration settings are fully documented, (2) re-emphasize compliance with operational procedures for ensuring server and desktop build procedures					

	are consistently applied for each operating system, and (3) evaluate the feasibility of adopting automated tool(s) that can facilitate periodic review of configuration settings to monitor compliance with build standards.	April 15, 2006	N/A	Yes	No	Open
Rec. Number	**Corrective Action: Taken or Planned/Status**	**Expected Completion Date**	**Monetary Benefits**	**Resolved:[a] Yes or No**	**Dispositioned:[b] Yes or No**	**Open or Closed[c]**
5	DIT will standardize a single system for tracking and documenting configuration changes and improving performance metric reporting.	August 31, 2006	N/A	Yes	No	Open

[a] Resolved – (1) Management concurs with the recommendation, and the planned corrective action is consistent with the recommendation.
(2) Management does not concur with the recommendation, but planned alternative action is acceptable to the OIG.
(3) Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Dispositioned – The agreed-upon corrective action must be implemented, determined to be effective, and the actual amounts of monetary benefits achieved through implementation identified. The OIG is responsible for determining whether the documentation provided by management is adequate to disposition the recommendation.

[c] Once the OIG dispositions the recommendation, it can then be closed.

DIVISION OF INFORMATION TECHNOLOGY COMMENTS

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500
Division of Information Technology

August 29, 2005

MEMORANDUM TO: Stephen M. Beard
Deputy Assistant Inspector General for Audits
Office of the Inspector General

FROM: Michael E. Bartell [Electronically produced version; original signed by Michael E. Bartell]
CIO and Director
Division of Information Technology

SUBJECT: DIT Response to the Draft Report Entitled Audit of FDIC's Information Technology Configuration Management Controls Over Operating System Software (Assignment No. 2005-004)

The Division of Information Technology (DIT) has reviewed the subject draft audit report and in general concurs with the Office of the Inspector General's (OIG) recommendations. Specific corrective actions and estimated completion dates for each recommendation are outlined below.

General Comments

DIT would like to thank the Inspector General for incorporating several changes discussed at the Exit Conference into this updated Draft Report. The updated Draft has addressed many of our initial concerns.

Responses to Recommendations

- Recommendation 1: Establish a policy that takes an enterprise approach to defining the roles, responsibilities, and overall principles and management expectations for performing configuration management on operating system software. The policy should address requirements for developing and maintaining configuration management plans and performing periodic self-assessments of configuration management processes and practices.

  Response: Partially Concur. DIT does agree that configuration management for operating systems is an area that should be covered by DIT policies. We do not believe that it is necessarily best to attempt to treat this issue within a single policy document covering all types of software. We agree to take a look at our policies to determine how most effectively to cover configuration management of the various operating systems and will develop appropriate modifications to existing policies or a new policy as required to meet the objectives of the recommendation. The new and/or revised policy will be established from a high-level, enterprise approach that will address requirements for configuration management plans and periodic self assessments. The new/revised policy will be approved and posted on the DIT Web site by November 30, 2005. (Infrastructure Services (Laterra), and Delivery Management (Livesay))

- Recommendation 2: Develop configuration management plan(s) covering the four operating system software platforms addressed in this report consistent with federal standards and guidelines and industry accepted practices. DIT should determine whether other operating system software platforms require configuration management plan(s) and develop such plans where appropriate.

  Response: Concur. While DIT does have procedures for configuring the servers indicated, DIT will formalize these into configuration management plans consistent with federal standards and guidelines for the four operating systems, as well as any other operating systems, by March 15, 2006. (Infrastructure Services (Laterra))

- Recommendation 3: Ensure that the certification and accreditation of the FDIC's general support systems incorporate an evaluation and testing of the FDIC's configuration management policy and plans referenced in recommendations 1 and 2 of this report.

  Response: Partially Concur. The FDIC's Security Test and Evaluation (ST&E) program, a component of the Certification and Accreditation (C&A) program, is currently testing using NIST 800-53 requirements to determine the level of compliance with NIST-specific guidance and industry best practices as they relate to configuration management policies, procedures, and plans. As new configuration management policy and procedures are implemented, DIT will include the evaluation and testing of updated policies to future C&A cycles, beginning in June 2006. (Information Security (Seborg))

- Recommendation 4: Document the minimum required configuration settings for the Windows® server and desktop operating system platforms and develop procedures to ensure that changes to baseline configuration settings are documented.

  Response: Partially Concur. DIT currently has several processes to document the required configuration setting for Windows® servers and desktop operating systems.

  DIT uses server build documents to detail the required hardware and software configuration settings for its Windows® servers. All server builds are based upon the build documents to ensure that minimum configuration settings are adhered to. Configuration settings supplied by the software manufacturer are modified as required for the FDIC technical requirements for each platform. In addition to the minimum configuration settings, additional settings, such as application specific SQL sort parameters, are also detailed in the build documents. When a server-related problem requires a configuration change, it is referred to Server Software. Server Software evaluates the issue to determine whether the proposed fix is needed. Once the fix is tested, approved and implemented, the server build is updated to reflect the fix and to ensure that all future builds incorporate the new configuration change. Significant exceptions to the standard build and reasons for the exception are documented as part of this process.

DIT will review the current procedures to ensure that the documentation will include the standard baseline configuration and approved exceptions to the configuration settings. We will also re-emphasize compliance with operational procedures established to ensure server and desktop build procedures are consistently applied for each operating system. Finally, DIT will investigate automated tools that may facilitate periodic review of configuration settings to monitor compliance with the standard build, and will implement the tool if it is determined to be beneficial. The required updates to documentation and related procedures, the management action to ensure procedural compliance with build standards and the investigation of possible automated tools for review of configuration settings will be completed by April 15, 2006. (Infrastructure Services (Laterra))

- Recommendation 5: Standardize and integrate the recording, tracking, and reporting of operating system software configuration changes to the maximum extent practical. As part of this effort, DIT should consider using automated mechanisms to improve performance metric reporting for configuration changes from a system-specific and enterprise perspective.

  Response: Concur. DIT has been working to standardize on a single system for tracking and documenting all configuration changes. This tool will provide improved performance metric reporting for configuration changes. The consolidation of the various systems into a single management tool will be completed by August 31, 2006. (Infrastructure Services (Laterra))

If you have any questions, please contact Rack Campbell, Chief ITES, on (703) 516-1422.

cc: Russell Pittman, DIT
Jerry Russomano, DIT
Ned Goldberg, DIT
Martha Adams, DIT
James Angel, OERM
Rack Campbell, DIT