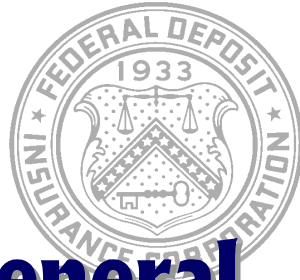


# Office of Inspector General



September 1, 2000  
Audit Report No. 00-038


---

**Audit of the Information Technology  
Configuration Management Program**



**DATE:** September 1, 2000

**TO:** Donald C. Demitros, Director  
Division of Information Resources Management

**FROM:**   
David H. Loewenstein  
Assistant Inspector General

**SUBJECT:** *Audit of the Information Technology Configuration Management Program (Audit Report No. 00-038)*

The Federal Deposit Insurance Corporation's (FDIC) Office of Inspector General (OIG) has completed an audit of the Information Technology Configuration Management (CM) Program. We initiated this audit to (1) evaluate the effectiveness and (2) assess the implementation of the FDIC's CM program policies and procedures. However, during the audit survey, we found that the FDIC's Division of Information Resources Management (DIRM) was in the process of developing a plan for establishing a more formal CM program. The purpose of this report is to provide our recommendations as to what DIRM should consider when developing the formal CM program. We recognize that DIRM management has already taken many positive steps in initiating the CM study, appears to have identified the critical issues in its CM efforts, and may independently develop similar conclusions and recommendations. Our purpose in presenting these recommendations is to emphasize what we feel are the salient features of an effective CM program. Once DIRM has developed, approved, and implemented a formal CM program, we will initiate an audit of the FDIC's implementation of the program.

## **BACKGROUND**

CM is a critical element in the development of hardware and software because it is the disciplined approach to controlling the inevitable changes that occur during a product's life cycle. CM controls product changes by providing the policies, procedures, and tools needed to preserve the product's history; ensuring that the product's components are uniquely identified; and controlling and evaluating a product's changes during its life cycle.

Our audit focused on the CM related to the FDIC's software inventory. The Institute of Electrical and Electronic Engineers' definition of software configuration management (SCM) includes four essential elements that are needed to maintain a product's integrity. These elements are:

- (1) **Configuration Identification.** The items of a system, such as requirements documents, specifications, design documents, source code, test suites, manuals, project plans, schedules, test plans, and procedural documents that must be identified, agreed upon, and established as the baseline from which changes will be measured.

- (2) **Configuration Control.** This is the method by which software changes and releases are controlled during the software life cycle. Any software changes and releases to the baselines must be documented and controlled through change requests.
- (3) **Configuration Accounting.** These are the CM activities that record and report the status of configuration items.
- (4) **Configuration Audit.** This is the process that verifies the completeness and correctness of a product's software baseline. In addition, any software changes must be verified for compliance with applicable standards and procedures.

During the life of a product, there are usually a myriad of changes that lead to the final configuration of the product. For this reason, these four elements need to be effectively controlled, tracked, and accounted for by automated CM tools. The use of such tools is particularly imperative when tracking the changes made during the software development process.

In recent years, the U.S. General Accounting Office (GAO) has repeatedly identified weaknesses in the CM of software in its reviews of federal agencies' information security programs. In recent correspondence to the Chairman of the House Subcommittee on Government Management, Information and Technology, the GAO concluded that based on its interviews with officials at 16 of the largest federal agencies, controls over changes to software for federal information systems as described in agency policies and procedures were inadequate. Because GAO identified government-wide weaknesses regarding software changes and related controls, it plans to recommend that the Office of Management and Budget (OMB) clarify guidance pertaining to these issues in its next revision to Circular A-130, *Management of Federal Information Resources*.

Presently, several branches within DIRM are engaged in CM activities. However, the FDIC does not yet have a formal CM program. During the FDIC's Year 2000 remediation efforts, the Corporation recognized that information technology policies were needed in such areas as CM and software testing. The FDIC has initiated a project to identify and recommend policies, procedures, and tools needed to support corporate software development efforts, including the establishment of formal CM practices, the enhancement of testing procedures, and the associated performance measurement activities.

To accomplish the FDIC's CM objectives, DIRM established the Configuration and Quality Management (CQM) group and detailed staff to develop the policies and procedures needed to implement a viable CM program. The project scope includes identifying and recommending the policies and procedures needed to govern CM, software testing, performance measurement, and software development. Presently, the staff is in the process of developing an action plan for accomplishing its project goals. The CQM staff expects to issue a report on its recommendations for implementing CM strategies by December 2000.

## **OBJECTIVES, SCOPE, AND METHODOLOGY**

The objectives of this audit were to evaluate the effectiveness of the FDIC's CM program policies and procedures and to assess the implementation of such policies and procedures.

To address our objectives, we reviewed CM program policies and procedures for compliance with GAO and OMB standards and generally accepted CM practices. We also reviewed the FDIC's use of CM tools to determine whether these tools were used for all the FDIC software. In addition to reviewing the CM process, we interviewed and held status meetings with responsible DIRM officials.

This audit was performed between March and July 2000 and conducted in accordance with generally accepted government auditing standards.

## **RESULTS OF AUDIT**

The FDIC has identified the need to improve its ability to control software changes through CM and has already recognized many of the issues noted in this report. We believe that DIRM should ensure that its CQM staff addresses the following issues as a more formal CM program is developed.

The FDIC needs to develop a centralized CM program that includes formal policies and procedures to control all software changes. Currently, administrative control over the development and modification of software is decentralized, and several DIRM offices perform CM activities. Further, DIRM does not yet have documented policies and procedures to ensure the establishment and implementation of (1) CM procedures for all the FDIC software changes, (2) controls over the labeling and inventorying of the FDIC software, and (3) criteria for the selection and use of CM tools.

Also, the FDIC would benefit from having a focal point to (1) ensure that all software changes are accounted for, (2) determine the overall impact of software changes on other FDIC operations, and (3) assess the cost-effectiveness of proposed software changes. This centralized control is needed to prevent (1) unauthorized software changes, (2) compromise of security features, (3) incorrect changes to software, and (4) noncompliance with GAO and OMB standards.

## **FDIC NEEDS TO DEVELOP AND DOCUMENT A CENTRALIZED CONFIGURATION MANAGEMENT PROGRAM**

DIRM does not currently have a centralized CM program that is controlled by formal policies, procedures, and specific roles and responsibilities. OMB Circular A-130, *Management of Federal Information Resources* (A-130), states: "agencies shall plan in an integrated manner for managing information throughout its life cycle." In addition, A-130 states: "agencies shall consider at each stage of the information life cycle, the effects of decisions and action on other stages of the life cycle." It also states: "agencies shall record, preserve, and make accessible sufficient information to ensure the management and accountability of agency programs, and to protect the legal and financial rights of the Federal Government." The GAO's *Federal Information System Controls Audit Manual* (FISCAM) states an entity should have a structured approach for controlling, identifying, and documenting changes in requirements that occur during the life of software from creation, development, product release, customer delivery, customer use, through the maintenance phase. FISCAM also states that software should be labeled and inventoried in a way that diminishes the risk that software will be misidentified or lost. The GAO's *Standards for Internal Control in the Federal Government* states: "Internal control systems and all transactions and other significant

events need to be clearly documented, and the documentation should be readily available for examination.” Also, the GAO *Standards for Internal Control in the Federal Government* states: “The documentation should appear in management directives, administrative policies or operating manuals and may be in paper or electronic form.”

During our review of current CM policies and procedures, we identified the need for a comprehensive CM program that documents the policies and procedures needed to ensure that (1) CM is initiated during the software development and modification process, (2) CM includes all the FDIC software, (3) the FDIC uses a standard method for labeling and inventorying all software, and (4) there is consistent selection and use of CM tools.

**DIRM Should Implement Configuration Management During the Software Development and Modification Process.** The current FDIC System Development Life Cycle (SDLC) Manual does not provide instructions or references to CM. In addition, the DIRM application and system developers we interviewed believe that they have no CM responsibilities during the software development and modification process. Therefore, we are concerned that the FDIC does not have adequate assurance that CM will occur during the software development and modification process. As a result, there is limited control or accountability for software changes made during the development and modification process.

**DIRM Needs to Ensure All FDIC Software Is Controlled by the Configuration Management Process.** Presently, DIRM does not use the CM process to control all FDIC software changes. In addition, the FDIC does not yet have a focal point responsible for (1) ensuring that all FDIC applications are under CM or (2) implementing the procedures on the use of CM tools. The lack of a formal CM program limits the FDIC's assurance that only authorized programs and authorized modifications are implemented. Without proper CM controls, security features may be circumvented and processing irregularities or unauthorized code may go undetected.

**DIRM Needs to Standardize the Labeling and Inventorying of FDIC Software.** Consistent labeling and inventorying of software is a key feature needed to control the CM process. We found, however, that in some cases the FDIC uses the same software acronyms to identify different software. In addition, although one CM tool had a documented inventory, the other CM tools in use did not have inventories that identified the software that they controlled. The inconsistent labeling and inventorying of software may result in difficulties in identifying needed software in a timely manner, or the selection of an incorrect version of software.

**DIRM Needs to Develop Policies and Procedures for the Consistent Selection and Use of Configuration Management Tools.** Presently, the DIRM application and system developers that we interviewed stated that they use their professional judgement when selecting a CM tool for software development and modification. In addition, we found that not all CM tools interface with each other. Without policies and procedures, DIRM will not be assured that CM tools are effectively selected and used.

## **CONCLUSION**

DIRM is in the initial stages of developing the policies and procedures for a comprehensive CM plan. When it reaches fruition, the project should greatly add to the control and effectiveness of the FDIC's software development process. During our review of the FDIC's configuration management policies and procedures, we identified enhancements to CM that the FDIC should consider when developing a formal CM program in the interest of ensuring the best possible program to control software changes during a product's life cycle.

## **RECOMMENDATION**

The Director, CQM should incorporate the following elements when developing the plan to implement a formal CM program at the FDIC.

The FDIC should establish a centralized CM program for information technology that includes documented policies, procedures, and responsibilities to ensure that (1) CM includes the entire software development and modification process, (2) all FDIC software is included in the CM program, (3) all FDIC software is subject to standardized labeling and inventorying process, (4) CM tools are consistently selected and used, and (5) the feasibility of integrating or consolidating the CM tools currently in use is explored.

## **CORPORATION COMMENTS AND OIG EVALUATION**

On August 24, 2000, the Director, DIRM, provided a written response to the draft report that concurred with the recommendation. These comments are included as appendix I. The Corporation's response to the draft report provides the elements necessary for management decisions on the report's recommendation.



Federal Deposit Insurance Corporation

3501 North Fairfax Drive, Arlington, VA 22226

Division of Information Resources Management

August 24, 2000

**TO:** David H. Loewenstein  
Assistant Inspector General

**FROM:** Donald C. Demitros  
Director, DIRM

**SUBJECT:** DIRM Management Response to the Draft OIG Report Entitled, "Audit of the Information Technology Configuration Management Program"

The Division of Information Resources Management (DIRM) has reviewed the subject draft audit report and generally agrees with the findings and recommendations.

One minor revision is requested. In the second paragraph of Page 4, the text should read "...Configuration and Quality Management (CQM) staff and detailed..."

The OIG's recommendation along with DRMS's response is provided below:

**OIG Recommendation:**

The Director, CQM should incorporate the following elements when developing the plan to implement a formal CM program at the FDIC.

The FDIC should establish a centralized CM program for information technology that includes documented policies, procedures, and responsibilities to ensure that (1) CM includes the entire software development and modification process, (2) all FDIC software is included in the program, (3) all FDIC software is subject to standardized labeling and inventorying process, (4) CM tools are consistently selected and used, and (5) the feasibility of integrating or consolidating the CM tools currently in use is explored.

**DIRM Response:**

DIRM has many controls in process but we concur that no centralized CM process exists which comprehensively covers all the controls mentioned in the OIG memo. The recommendation from the CQM Staff to DIRM senior management will include a comprehensive, long-term plan to implement a CM program that addresses these concerns.

CQM will also recommend a prioritized schedule for implementing such a program that will

focus first on software version control, change control, and a rigorous testing methodology. Additional elements of the program proposal will include recommendations for the development of thorough policies and procedures and the development, publication and implementation of a defined methodology in a deliberate and disciplined fashion.

DIRM will complete the formal process and methodology by December 31, 2000.

If you have any questions, please contact Rack Campbell, DIRM's Audit Liaison, at (703) 516-1422.

cc: Vijay Deshpande, OICM  
Larry Proctor, DIRM



**MANAGEMENT RESPONSES TO RECOMMENDATIONS**

The Inspector General Act of 1978, as amended, requires the OIG to report the status of management decisions on its recommendations in its semiannual reports to the Congress. To consider FDIC’s responses as management decisions in accordance with the act and related guidance, several conditions are necessary. First, the response must describe for each recommendation

- the specific corrective actions already taken, if applicable;
- corrective actions to be taken together with the expected completion dates for their implementation; and
- documentation that will confirm completion of corrective actions.

If any recommendation identifies specific monetary benefits, FDIC management must state the amount agreed or disagreed with and the reasons for any disagreement. In the case of questioned costs, the amount FDIC plans to disallow must be included in management’s response.

If management does not agree that a recommendation should be implemented, it must describe why the recommendation is not considered valid. Second, the OIG must determine that management’s descriptions of (1) the course of action already taken or proposed and (2) the documentation confirming completion of corrective actions are responsive to its recommendations.

This table presents the management responses that have been made on recommendations in our report and the status of management decisions. The information for management decisions is based on management’s written response to our report.

<b>Rec. Number</b>	<b>Corrective Action: Taken or Planned/Status</b>	<b>Expected Completion Date</b>	<b>Documentation That Will Confirm Final Action</b>	<b>Monetary Benefits</b>	<b>Management Decision: Yes or No</b>
1	CQM staff will develop a comprehensive, long-term plan to implement a CM program that addresses the OIG’s concerns. CQM staff will also recommend a prioritized schedule for implementing the program.	12/31/2000	Final CM Plan	Not Quantifiable	Yes