Office of Inspector General

January 2, 2002
Audit Report No. 02-001

Follow-up Audit of Internal Controls Over the Customer Information and Control System for the FDIC Financial Systems

FDIC
Federal Deposit Insurance Corporation
Washington, D.C. 20434

Office of Audits
Office of Inspector General

DATE: January 2, 2002

TO: Carol M. Heindel, Acting Director,
Division of Information Resources Management

FROM: Russell A. Rau [Electronically produced version; original signed by Russell A. Rau]
Assistant Inspector General for Audits

SUBJECT: Final Report Entitled *Follow-up Audit of Internal Controls over the Customer Information and Control System for FDIC Financial Systems*
(Audit Report No. 02-001)

This report presents the results of our follow-up audit of internal controls over the Customer Information and Control System (CICS). Our objectives were to evaluate the adequacy of the installation parameters[1] used by the CICS system software for the financial systems and the adequacy of access security over CICS files, resources,[2] and software monitoring products.[3] Our audit scope and methodology are discussed in Appendix I.

Previously, we conducted an audit that included all of the CICS system controls, including the installation parameters used by the CICS system software for the financial systems and the adequacy of access security over CICS files, resources, and software monitoring products. On June 19, 1997, we issued a report entitled *CICS for the IBM and Amdahl Mainframe Computers*. The report included recommendations for further protecting the integrity and performance of application programs under CICS, improving access controls, and reducing the risk of CICS authorizations for a given application system interfering with or bypassing the security mechanisms for other application systems under CICS control. Appendix II contains a summary of the recommendations and management comments in that report.

INTRODUCTION

CICS is a transaction management program for mission-critical applications, such as the Bank Information Tracking System, Call Processing System, and the FDIC's financial systems. The

[1] Data (in files) or code that can be used to designate how systems are initiated. Parameters include limits on operator intervention, periodic file back-ups, and security options.
[2] Resources are transactions, applications, terminal devices, and communications.
[3] Software monitoring products are vendor supplied programs that allow systems engineers to detect and correct inefficiencies or errors in computer operations.

FDIC's financial systems include the Financial Information Management System general ledger, the Accounts Payable Purchase Order System, and the Electronic Procurement Routing Invoice Solution. The financial systems record and report all the financial activity of the Corporation.

CICS provides the interface between these application programs and the computer's operating system. Specifically, it provides the mainframe operating system with the ability to handle transactions from user terminals such as a personal computer. For example, a transaction sent from a personal computer could be a user processing an accounting entry. CICS interprets the user command to process the accounting entry, calls the appropriate application program, and passes the user information to that program. Once the program is finished, CICS passes any response from the application program back to the user's personal computer. In almost all application program environments, CICS involvement in the communications and tracking process is transparent to the end user.

In order to conduct these functions, CICS utilizes a System Definition File. The System Definition File within CICS identifies and defines what transactions or programs are available to users of the mission-critical applications. Also, the CICS software system includes very powerful capabilities (e.g., commands that can shut down the application systems) that must be appropriately controlled to protect corporate applications and data. Consequently, to ensure the integrity of application programs and data, CICS must be integrated with the security software used on the mainframe computer.

RESULTS OF AUDIT

Controls were not in place to protect access to the CICS System Definition File within the CICS system. As a result, over 100 non-CICS programmers had full access to the System Definition File and had the capability to shut down or disrupt the systems that are critical to the FDIC's mission. This condition was brought immediately to the attention of DIRM management who took appropriate action to correct the problem.

Our evaluation of the installation parameters for the CICS system showed that the parameters used in activating the financial systems were consistent with guidelines and recommendations provided by the product's vendor.[4] We also concluded that other access security controls were adequate for CICS system files, resources, and software monitoring products used by the FDIC financial systems.

ACCESS TO CICS SYSTEM DEFINITION FILE

Over 100 non-CICS programmers had full access to the CICS System Definition File. They had read, write, and execute capabilities when only the duties of CICS system programmers require this level of access. Access rules[5] that were in place to limit the number of programmers with access to the CICS System Definition File and its maintenance program were negated when the FDIC installed new broad access rules within the security program to permit programmers to access less sensitive

[4] The vendor for CICS is International Business Machines, Incorporated.

[5] Access rules are instructions coded into a security system to designate which users are allowed access to systems and information.

systems and information. Upon accessing the System Definition File, programmers had the capability to shut down or disrupt the systems that are critical to the FDIC's mission. Consequently, excessive access and authority to modify software increases the risk that unapproved changes can be made that could compromise data integrity, accuracy, and availability.

Background

Office of Management and Budget Circular A-130, Appendix III, section B.(a) 2. (c) states

> In every general support system, a number of technical, operational, and management controls are used to prevent and detect harm. Such controls include individual accountability, "least privilege," and separation of duties. Least privilege is the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job.

Also, FDIC Circular 1360.15 requires the protection of sensitive automated information systems and data from unauthorized access, disclosure, and use. Sensitive information systems include those systems that process financial information and data protected from disclosure by any applicable law, regulation, or order.

Adequacy of Access Controls

Over 100 non-CICS programmers had the capability to read, write, and execute commands to the CICS System Definition File. However, only the duties of CICS system programmers require this level of access. CICS programmers require read, write, and execute access in order to perform routine system maintenance. The non-CICS programmers with access to the System Definition File had responsibilities that were not related to CICS or the System Definition File.

Access rules that were in place to limit the number of programmers with access to the CICS System Definition File and its maintenance program were negated when the FDIC installed new broad access rules within the security program to permit programmers to access less sensitive systems and information. The new broad access rules superceded all other rules, including the specific access rules to limit access to the CICS System Definition File. A broad access rule will supercede all other rules unless a rule is installed that explicitly denies access to specific systems and information. Consequently, the broad access rules designated multiple non-CICS programmers with the capability to access the sensitive CICS System Definition File.

These non-CICS programmers had the capability to shut down or disrupt the critical FDIC systems. For instance, each of the programmers had the ability to access a maintenance program and modify user group definitions within the System Definition File. This would permit the programmers to add themselves or others to a user group that is authorized to execute powerful CICS system commands such as the CICS master terminal transaction (CEMT) used to shut down the CICS system at any time. Upon executing the CEMT command and shutting down CICS, other users would not be able to enter commands or transactions to the financial systems, Bank Information Tracking System, or any of the other critical systems. As a result, the risk of this occurrence or other disruptions

increases as the number of users with full access to the System Definition File increases.

This condition also existed during our previous audit, and it was included in our report, *CICS for the IBM and Amdahl Mainframe Computers*, dated June 19, 1997. To resolve that finding, DIRM implemented Access Rules to limit the access to four CICS programmers. However, the access rules implemented were overridden by additional changes made since that time.

Recommendations

We recommend that the Acting Director, DIRM:

(1) strictly limit access to the CICS System Definition File and its maintenance program to CICS programmers with responsibilities that warrant that access and
(2) implement access rules to ensure that future changes to the security database do not inadvertently negate the access rules intended for the CICS System Definition File and its maintenance program.

CORPORATION COMMENTS AND OIG EVALUATION

We notified FDIC officials of our finding during the fieldwork phase of our audit. They responded by installing security restrictions that allow only four CICS Systems Programmers to have full read, write, allocate, and execute access. Further, three other system programmers for the mainframe operating system will have only read and execute access to the CICS System Definition File. FDIC officials replied that additional precautions have been implemented to ensure that these specific security changes cannot be overridden[6] and that the new changes have been documented to indicate the need for restricted access. Later, on December 20, 2001, we provided our draft report to the Acting Director of DIRM and her office responded that they had no further comments.

FDIC actions during the audit were responsive to our recommendations. In addition, we determined through our review of the applicable mainframe files that corrective actions had been completed and were effective. The two recommendations in our report are closed for reporting purposes.

[6] DIRM installed "prevent rules" for the CICS System Definition and utility files. Prevent rules instruct the security system to ignore any other broad access rules that do not specifically address these files.

APPENDIX I

Scope and Methodology

The audit scope focused on the CICS controls that control transactions for the financial application systems, and we reviewed the security of other systems that share files or communicate with the financial systems to ensure that such arrangements did not bypass controls over the financial systems. We reviewed the installation commands (job control language) and CICS installation parameters. We determined the identity of installation files for the CICS and the financial systems and evaluated the contents of all files by directly accessing the mainframe computer. Installation commands and parameters were evaluated using the recommended procedures contained in the vendor's publications.

We also reviewed access security over files and resources, intersystem communications, and the interfaces between CICS and products used to secure and monitor CICS resources. We conducted tests of CICS and vendor transaction commands such as those used in modifying user capabilities. Selected commands were tested on the financial systems to verify that proper access security controls were functioning, and we used vendor-supplied utilities to ascertain the types of access available to critical files and resources. We obtained a copy of the CICS System Definition File and evaluated the resources available to users of the financial systems and the extent of communication allowed with other corporate systems.

We conducted our audit from June 4, 2001 to August 15, 2001 in accordance with generally accepted government auditing standards.

APPENDIX II

Prior Audit Report entitled *CICS for the IBM and Amdahl Mainframe Computers*, dated June 19, 1997

Summary of Recommendations and Management Comments

Our audit report presented 14 recommendations for further protecting the integrity and performance of application programs under CICS, improving access controls, and reducing the risk of CICS authorizations for a given application system interfering with or bypassing the security mechanisms for other application systems under CICS control.

- Protection of the integrity and performance of the application programs under CICS

  The report recommended changes to the sequence of installing the security programs and CICS parameters during the system start-up. We also recommended the elimination of unnecessary files that were included in the system start-up, implementation of the security controls used to protect powerful system programs, and the standardization and centralization of CICS resources.

- Adequate access controls

  Recommendations addressed improvements in controlling access to the CICS System Definition Files and to the maintenance programs that service these files, restricting the number of users with access to powerful CICS system and third-party vendor transactions/utility program libraries, and preventing users from using unsecured sign-on screens.

- Reduce the risk of CICS authorizations for a given application system interfering with or bypassing the security mechanisms for other application systems under CICS control

  Recommendations included eliminating the use non-production files in a production application and removing the communication links from one CICS production system to a non-production system.

Management concurred with all 14 recommendations and implemented corrective actions to address the cited deficiencies.