

AUDIT REPORT



CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
BUREAU OF FINANCIAL AUDIT
WILLIAM C. THOMPSON, JR., COMPTROLLER

Audit Report on the User Access Controls of the Financial Management System at the Financial Information Services Agency

7A03-137

June 25, 2003



THE CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
1 CENTRE STREET
NEW YORK, N.Y. 10007-2341

WILLIAM C. THOMPSON, JR.
COMPTROLLER

To the Citizens of the City of New York

Ladies and Gentlemen:

In accordance with the Comptroller's responsibilities contained in Chapter 5, § 93, of the New York City Charter, my office has performed an audit on the user access controls of the Financial Management System at the Financial Information Services Agency. The results of our audit, which are presented in this report, have been discussed with officials from the Financial Information Services Agency, and their comments have been considered in preparing this report.

Audits such as this provide a means of ensuring that the City has adequate controls in place to protect its records from unauthorized access.

I trust that this report contains information that is of interest to you. If you have any questions concerning this report, please contact my audit bureau at 212-669-3747 or e-mail us at audit@Comptroller.nyc.gov.

Very truly yours,

A handwritten signature in cursive script that reads 'William C. Thompson, Jr.'.

William C. Thompson, Jr.

WCT/GR

Report: **7A03-137**
Filed: **June 25, 2003**

Table of Contents

Audit Report In Brief	1
Audit Findings and Conclusions	1
Audit Recommendations	2
Introduction	2
Background	2
Objectives	3
Scope and Methodology	3
Discussion of Audit Results	4
Findings and Recommendations	5
Log Not Maintained	5
Periodic Training Not Provided to FMS Security Officers	6
Addendum – FISA Response	7

*The City of New York
Office of the Comptroller
Bureau of Financial Audit*

**Audit Report on the
User Access Controls of the
Financial Management System at the
Financial Information Services Agency**

7A03-137

AUDIT REPORT IN BRIEF

We performed an audit on the user access controls of the Financial Management System (FMS) at the Financial Information Services Agency (FISA). FISA is responsible for data processing operations that support the activities of City personnel and units responsible for organizing, compiling, and coordinating the City's central financial records, data, and related information and for making appropriate reports. FISA provides authorized access to information stored in FMS. FMS, which was implemented in June 1999, is the City's centralized accounting and budgeting system, supported by FISA from its mainframe computers. FISA permits personnel access to FMS based on approval by each respective agency.

Currently, some 3,500 users from more than 90 City agencies have access to FMS. FISA handles the processing of new FMS user requests through more than 200 agency FMS security officers who are chosen by their respective agencies.

Audit Findings and Conclusions

FISA has adequate controls in place to protect FMS records from unauthorized access. Specifically, FISA:

- Established formal security procedures and included them in its *Agency FMS Administration Policies & Procedures* statement;
- Maintains electronic and manual hard-copy records for special FMS access requests;
- Requires that agencies designate a FMS security officer and a backup FMS security officer who are familiar with the agency's mission and how it relates to FMS;
- Requires adequate separation of duties over user access to different components of FMS.

- Provides protection against unauthorized access by automatically revoking access to FMS when user identification (ID) codes are used with invalid passwords;
- Revokes ID codes of users not properly accessing FMS for a 30-day period.

However, although we found that FISA maintains electronic and manual hard-copy records for special FMS access requests and the corresponding approvals or rejections, FISA does not maintain a central log of those requests. In addition, FISA does not provide periodic training to FMS security officers.

Audit Recommendations

To address these issues, FISA should:

- Establish a log to record all requests from agencies for special FMS access rights.
- Provide periodic training to FMS security officers.

INTRODUCTION

Background

The Financial Information Services Agency (FISA) is responsible for data processing operations that support the activities of City personnel and units responsible for organizing, compiling, and coordinating the City's central financial records, data, and related information and for making appropriate reports. Three directors appointed by the Mayor oversee FISA (one of the directors is appointed upon the recommendation of the Comptroller). FISA provides access to information needed by the City personnel and units that determine and administer estimated and actual City expenditures; the receipt, investment and disbursement of City funds; and the issuance and payment of principal and interest on City obligations. FISA is also responsible for the implementation and processing of the City Payroll Management System.

FISA provides authorized access to information stored in the City Financial Management System (FMS) and its Payroll Management System (PMS). Access is authorized for City personnel responsible for: (1) administration of the City budget; (2) accounting of City funds; (3) procurement of goods and services required by City agencies; and (4) City payroll and personnel information. FMS, which was implemented in June 1999, is the City's centralized accounting and budgeting system, supported by FISA from its mainframe computers. FISA permits personnel access to FMS based on approval by each respective agency.

Currently, some 3,500 users from more than 90 City agencies have access to FMS. FISA handles the processing of new FMS user requests through more than 200 agency FMS security officers who are chosen by their respective agencies.

Objectives

This audit's objective was to determine whether adequate controls are in place to protect FMS records from unauthorized access.

Scope and Methodology

Our fieldwork was conducted between February 2003 and April 2003. To achieve our objective, we interviewed FISA officials, reviewed FMS background material, FISA policies and procedures, and listings of FMS users and user agencies. We also reviewed City payroll records to verify whether all individuals designated as security officers were current City employees.

Deloitte & Touche LLP is the City's external auditor. We reviewed and relied upon its Report to Management for the year ended June 30, 2002 (dated October 28, 2002), as it related to our audit objectives.

It should be noted that our audit focused on operations and controls of FMS within FISA, and on FISA procedures, controls, and authority governing the FMS application. We did not review or test FMS-related controls at the individual City agency level. These controls are outside the scope of our current audit.

To meet our audit objectives, we used Comptroller's Internal Control and Accountability Directive 18, *Guidelines for the Management, Protection and Control of Agency Information and Information Processing Systems*, as a criterion for this audit. In addition, we reviewed relevant sections of the New York City Charter.

Independence Disclosure

In accordance with Chapter 38, § 860, of the New York City Charter, one of the three FISA directors is appointed upon the recommendation of the Comptroller. The directors are responsible for recommending an executive director, who is appointed by the Mayor. The director recommended by the Comptroller was not involved in planning or conducting this audit, or in writing or reviewing the audit report prior to its publication.

This audit was conducted in accordance with generally accepted government auditing standards (GAGAS) and included tests of the records and other auditing procedures considered necessary. This audit was performed in accordance with the audit responsibilities of the City Comptroller as set forth in Chapter 5, § 93, of the New York City Charter.

Discussion of Audit Results

The matters covered in this report were discussed with FISA officials during and at the conclusion of this audit. A preliminary draft was sent to FISA officials and discussed at an exit conference held on June 5, 2003. On June 10, 2003, we submitted a draft report to FISA officials with a request for comments. We received a written response from the Department on June 16, 2003, in which FISA indicated that it has established, and is using a log to record agency requests for special FMS access rights and has implemented periodic training for FMS security officers.

The full text of FISA's comments is included as an Addendum to this report.

FINDINGS AND RECOMMENDATIONS

FISA has adequate controls in place to protect FMS records from unauthorized access. Specifically, FISA:

- Established formal security procedures and included them in its *Agency FMS Administration Policies & Procedures* statement;
- Maintains electronic and manual hard-copy records for special FMS access requests;
- Requires that agencies designate a FMS security officer and a backup FMS security officer who are familiar with the agency's mission and how it relates to FMS;
- Requires adequate separation of duties over user access to different components of FMS.
- Provides protection against unauthorized access by automatically revoking access to FMS when user identification (ID) codes are used with invalid passwords;
- Revokes ID codes of users not properly accessing FMS for a 30-day period.

However, although we found that FISA maintains electronic and manual hard-copy records for special FMS access requests and the corresponding approvals or rejections, FISA does not maintain a central log of those requests. In addition, FISA does not provide periodic training to FMS security officers. These issues are discussed in greater detail in the following sections of this report.

Log Not Maintained

FISA maintains email or hard-copy records of requests for additional or special FMS access rights, and records of request approvals and rejections. However, FISA does not maintain a log of such requests and dispositions. A log that records all requests for additional or special FMS access rights would create an easy audit trail for tracking any FMS security infractions. At a minimum, the log should contain:

- **Request Date** – The date of the initial request for special access rights to FMS.
- **Agency** – Name of the City agency making the request.
- **Requesting FMS security officer** – Name of the agency FMS security officer making the request on behalf of his or her agency.
- **Brief Description of Request** – Describe why the special access to FMS is needed.

- **Action Taken (approved or rejected)** – Record whether the request was approved or rejected.
- **Action Date** – The date action was taken, or effective date of approved special access to FMS.

Comptroller’s Directive 18 § 8.5 states:

“A key element in the control over the information processing environment is the incorporation of audit trails into general and application control procedures. Audit trails maintain records of a variety of system events and activities. Every data entry or change, all modifications of system software or application software, and changes in the authorized use of a system’s physical resources should result in the recordation of the event so that management or auditors can trace any change back to its source.”

Recommendation

1. FISA should establish a log to record all requests from agencies for special FMS access rights.

FISA Response: “FISA has established a log to record all requests from agencies for special FMS access rights. Use of the log has already been implemented”

Periodic Training Not Provided to FMS Security Officers

FISA does not provide periodic training to FMS security officers. In fact, the only training provided to the officers was given at the time FMS was implemented. Since the security officers provide a critical role in ensuring that only authorized individuals have access to the system it is important that they receive appropriate training. Such training also ensures that new FMS security officers have the knowledge required to perform their responsibilities.

Recommendation

2. FISA should provide periodic training to FMS security officers.

FISA Response: “FISA agrees with this recommendation and will implement periodic training. The first training session will be held in August, 2003. Thereafter, training will take place semi-annually.”



The City of New York
Financial Information Services Agency

450 West 33rd Street, 4th Floor
New York, NY 10001-2603

Telephone: (212) 857-1200
Fax: (212) 857-1106
TTY: (212) 857-1780

MICHAEL R. BLOOMBERG, *Mayor*
WILLIAM C. THOMPSON, JR., *Comptroller*

ROBERT W. TOWNSEND
Executive Director

June 16, 2003

Mr. Gary Rose
Director of Financial Audits
Office of the Comptroller
Bureau of Audits
1 Centre Street, Room 1300 North
New York, NY 10007

**Re: Audit Report on the User Access Controls of the
Financial Management System at the Financial
Information Services Agency 7A03-137**

Dear Mr. Rose:

The Financial Information Services Agency has reviewed the observations and recommendations listed in the Comptroller's Office Draft Audit Report dated June 10, 2003. The following represents FISA management responses to the observations and recommendations listed in the report.

FISA MANAGEMENT RESPONSE

1. **Log Not Maintained**

FISA maintains e-mail or hard-copy records of requests for additional or special FMS access rights, and records of request approvals and rejections. However, FISA does not maintain a log of such requests and dispositions. A log that records all requests for additional or special FMS access rights would create an easy audit trail for tracking any FMS security infractions. At a minimum, the log should contain:

- **Request Date** – The date of the initial request for special access rights to FMS.

Mr. Gary Rose
Page 2
June 16, 2003

- **Agency** – Name of the City agency making the request.
- **Requesting FMS security officer** – Name of the agency FMS security officer making the request on behalf of his or her agency.
- **Brief Description of Request** – Describe why the special access to FMS is needed.
- **Action Taken (approved or rejected)** – Record whether the request was approved or rejected.
- **Action Date** – The date action was taken, or effective date of approved special access to FMS.

Comptroller's Directive 18 § 8.5 states:

“A key element in the control over the information processing environment is the incorporation of audit trails into general and application control procedures. Audit trails maintain records of a variety of system events and activities. Every data entry or change, all modifications of system software or application software, and changes in the authorized use of a system's physical resources should result in the recordation of the event so that management or auditors can trace any change back to its source.”

Recommendation

FISA should establish a log to record all requests from agencies for special FMS access rights.

Management's Response

FISA has established a log to record all requests from agencies for special FMS access rights. Use of the log has already been implemented.

2. **Periodic Training Not Provided to FMS Security Officers**

FISA does not provide periodic training to FMS security officers. In fact, the only training provided to the officers was given at the time FMS was implemented. Since the security officers provide a critical role in ensuring that only authorized individuals have access to the system it is important that they receive appropriate training. Such training also ensures that new FMS security officers have the knowledge required to perform their responsibilities.

Mr. Gary Rosc
Page 2
June 16, 2003

Recommendation

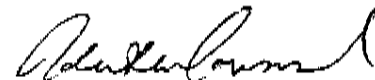
FISA should provide periodic training to FMS security officers.

Management's Response

FISA agrees with this recommendation and will implement periodic training. The first training session will be held in August, 2003. Thereafter, training will take place semi-annually.

If you have any questions on these comments, please direct them to Ms. Adele Croce at (212) 857-1113.

Sincerely,



Robert W. Townsend
Executive Director

cc: R. Fuchs
J. Festa
D. Pascali
A. R. Edley
A. Croce