The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DeNUCCI
AUDITOR

TEL. (617) 727-6200

No. 2007-0701-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE MALDEN HOUSING AUTHORITY

October 1, 2005 through February 28, 2007

OFFICIAL AUDIT REPORT

JUNE 25, 2007

TABLE OF CONTENTS

INTRODUCTION

The Malden Housing Authority (MHA), which was established through Chapter 121B, Section 3 of the Massachusetts General Laws, provides for the construction, acquisition, rehabilitation and management of rental housing for low-income persons residing in Malden, Massachusetts. A five-member Board of Directors, one of whom is appointed by the Governor and four who are appointed by the Mayor of the City of Malden, including one tenant representative, governs the MHA. The MHA is comprised of seven departments; administration, finance, maintenance, leased housing, modernization, support services, and tenant services. The MHA operates from a central office located in Malden at 630 Salem Street and manages eight development sites throughout the city. At the time of our audit, approximately 57 employees staffed the MHA.

The MHA's primary mission is to provide stable, affordable housing for low and moderate-income persons and to create an environment for individuals to transform from dependency to economic self-sufficiency. The MHA is comprised of approximately 1,984 public housing units, of which 429 are state housing and 1,555 are federal housing. The MHA state-funded units consist of family and elderly/disabled housing and housing for special needs. The MHA federally funded units consist of the Federal Conventional Elderly Housing Program, which has approximately 987 housing units or 49.7% of MHA housing units. In addition, the Authority manages rental assistance programs, such as the Federal Section 8-Voucher Program and the state-funded Massachusetts Rental Voucher Program, which help provide tenants access to affordable housing in non-MHA owned properties. Through the rental assistance programs, the MHA administers approximately 584 rental assistance vouchers. Of the 584 vouchers, 559 represent the vouchers for the MHA and the remaining 25 are administered by the MHA for other housing authorities. The MHA is governed by housing regulations issued by the United States Department of Housing and Urban Development (HUD) and the Massachusetts Department of Housing and Community Development (DHCD).

For the annual fiscal period ending September 30, 2005, the MHA received $13,263,944, in federal operating subsidy and grants as well as $236,764 for state funded grants. In addition, the MHA reported shelter rental income for both federal and state programs totaling $6,025,186 for that period. The MHA expects the Independent Public Accountant (IPA) single audit of the MHA for fiscal year ending September 30, 2006 to begin approximately in April 2007.

At the time of our audit, MHA computer operations consisted of 22 microcomputer workstations and two laptop computers located at the MHA central office and the development sites. The MHA uses two file servers to support a local area network (LAN) and a wide area network (WAN). The MHA has a total of two IT staff members, one of whom is part-time.

The MHA's primary software application is the HAB system from the vendor Hawkins, Ash and Baptie, Inc. of LaCrosse, Wisconsin. The application provides data processing functions using a module-based system for multiple housing authority functions. The HAB system contains a general ledger function, which is used primarily by MHA's fee accountant. In addition, the MHA uses a separate Windows-based application system for processing administrative functions including fixed-asset inventory, rental information, and tenant applications.

The Office of the State Auditor's audit consisted of an examination of certain IT general controls over and within the MHA's IT environment, a review of the type of data entered and stored in the HAB application for the Federal Conventional Elderly Housing Program, and a review of controls to protect the confidentiality of hardcopy records.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From November 30, 2006 through February 28, 2007 we performed an audit of selected information technology (IT) related controls at the Malden Housing Authority (MHA) for the audit period of October 1, 2005 through February 28, 2007. The scope of our audit included an evaluation of IT-related controls pertaining to physical security, environmental protection, system access security, inventory control over IT-related assets, disaster recovery and business continuity planning, and on-site and off-site storage of backup copies of magnetic media. In addition, we assessed controls over the security and disposal of confidential records; and reviewed the types of data stored in the HAB application system for the Federal Conventional Elderly Housing Program. Our evaluation of controls for access security did not include security controls pertaining to Internet access.

Audit Objectives

Our primary objective was to determine whether adequate controls were in place and in effect for selected IT functions in the Authority's processing environment. We sought to determine whether the MHA's IT-related internal control framework, including policies, procedures, practices, and organizational structure, provided reasonable assurance that IT-related control objectives would be achieved to support business functions. We sought to determine whether adequate physical security and environmental protection controls were in place and in effect to prevent unauthorized access, damage to, or loss of IT-related assets. Our objective regarding system access security was to determine whether adequate controls were in place to ensure that only authorized personnel had access to the MHA's automated systems. Further, we sought to determine whether MHA management was monitoring password administration.

We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that IT-related assets were properly recorded and accounted for and were safeguarded against unauthorized use, theft, or damage. We also determined whether the MHA had an effective business continuity plan that would provide reasonable assurance that mission-critical and essential IT-related operations could be regained within an acceptable period of time should the computerized functions be rendered inoperable or inaccessible. In addition, we sought to determine whether the MHA had adequate procedures for on-site and off-site storage of backup copies of magnetic media to support system and data recovery objectives. A further objective was to determine whether adequate controls over the security and disposal of confidential records was being exercised at the MHA to meet the regulations promulgated by the Office of the Secretary of Commonwealth.

Audit Methodology

To determine the audit scope and objective, we conducted pre-audit work that included obtaining and recording an understanding of relevant operations, performing a preliminary review and evaluation of certain IT-related internal controls, and interviewing senior personnel. We interviewed senior management during pre-audit regarding organizational controls and management practices, such as documented policies and procedures, job descriptions, and organizational structure. To obtain an understanding of the internal control environment, we reviewed the MHA's primary business functions and stated controls. We obtained an understanding of the Authority's mission-critical software application system modules. We performed a high-level risk analysis and assessed the strengths and weaknesses of the internal control system for selected activities, and upon completion of our pre-audit work, we determined the scope and objectives of the audit.

To evaluate physical security, we interviewed management and security personnel, conducted a walk-through, observed security devices, and reviewed procedures to document and address security violations and/or incidents. Through observation, we determined the adequacy of physical security controls over the file server room, office areas, and the off-site storage area. We examined the existence of controls, such as office door locks, remote cameras, and intrusion alarms. We determined whether individuals identified as being authorized to access areas housing computer equipment were current employees of the MHA and that the areas were restricted to only authorized personnel.

To determine the adequacy of environmental protection controls, we conducted a walk-through and evaluated controls within the file server room and the off-site storage area. We examined the areas housing IT equipment at the MHA to determine whether IT resources were subject to adequate environmental protection. Our examination included a review of general housekeeping; fire prevention, detection, and suppression; heat detection; uninterruptible power supply; emergency lighting and shutdown procedures; water detection; and humidity and air conditioning control. Audit evidence was obtained through interviews, observation, and review of relevant documentation.

Our tests of system access security included a review of procedures used to authorize, activate, and deactivate access privileges to the local area network and application systems. To determine whether only authorized employees were accessing the automated systems, including the HAB system, we obtained a system user list from MHA for individuals granted access privileges to the automated systems and compared it to the current personnel listing. We tested access accounts for 100% of the MHA's HAB systems access users and e-mail users as of January 31, 2007. Our examination consisted of a review of all 27 HAB systems access users and all 24 e-mail users. We reviewed control practices regarding logon ID and password administration by evaluating the extent of documented policies and guidance provided to the MHA personnel. We determined whether all employees authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes. We review control practices for password composition, length, and restrictions on the reuse of passwords. In addition, we reviewed the supervisory level access privileges.

To determine whether adequate controls were in place and in effect to properly safeguard and account for computer equipment, we reviewed inventory control procedures for property and equipment, obtained a copy of the inventory system of record, reviewed the types of data contained in the inventory, and performed inventory tests. We examined policies and procedures regarding fixed-asset inventory to determine whether the MHA was in compliance with regulations and generally accepted inventory control practices. We tested 100% of the MHA’s December 31, 2006 inventory of computer equipment for 31 IT-related items to assess the accuracy, completeness and verifiability of inventory data including identification tag number, location, description, and historical cost. Our examination of MHA’s inventory of computer equipment consisted of examining information pertaining to desktop computers, laptop computers, printers, and the file servers. We also obtained an understanding of the MHA’s acquisition and disposition process for computer equipment.

To assess the adequacy of business continuity planning, we determined whether any formal planning had been performed to resume computer operations should the network application systems be inoperable or inaccessible. In addition, we determined whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. Further, to evaluate the adequacy of controls to protect data files through the generation and on-site and off-site storage of backup copies of magnetic media and hardcopy files, we interviewed MHA staff and inspected the on-site backup location. We also assessed the status of the MHA’s record retention and disposition procedures by conducting interviews with MHA employees.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States and generally accepted industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT), as issued by the Information Systems Audit and Control Association, July 2004.

AUDIT CONCLUSION

Based on our audit at the Malden Housing Authority, we determined that internal controls in place provided reasonable assurance that IT-related control objectives pertaining to physical security, environmental protection, the accounting of IT resources, systems access security, and the disposing of confidential records would be met. However, controls over business continuity planning needed to be strengthened since there was no disaster recovery strategy in place nor was there a formalized, approved business continuity plan.

We found that the MHA had adequate physical security controls in place to provide reasonable assurance that only authorized persons could access the file server room and other areas housing IT equipment. In addition, our audit confirmed that other physical security controls were in place at the eight development sites and that access to the individual business offices at the various sites was restricted to MHA personnel.

Adequate environmental protection was found to be in place to provide reasonable assurance that IT resources would be protected from damage or loss. Specifically we determined that controls, such as temperature controls, smoke detectors, fire alarms, hand-held fire extinguishers, and an uninterruptible power supply were in place in the file server room to prevent damage to, or loss of, IT resources. We found that the file server room and other areas housing IT equipment were neat, clean, and in good order. We recommend, however, that the MHA management post emergency shut down procedures in the file server room and evacuation procedures at the development sites.

With respect to system access security, our audit disclosed that the process for granting and recording authorization and activating logon IDs and passwords was appropriate. We noted that control practices regarding access security policies and procedures for periodic changes to passwords were in place and in effect. Our audit indicated that passwords were being changed periodically and that there were requirements for password composition. We recommend that MHA develop and formalize written and approved policies and procedures pertaining to systems access security usage. Overall, we determined that appropriate controls were in place to provide reasonable assurance that control objectives related to user account management would be addressed.

With respect to IT-related fixed-asset inventory control, we found that the MHA was adhering to the policies and procedures promulgated by Department of Housing and Community Development. Based upon a review of 100% of the Authority's IT-related items, as listed on MHA's December 31, 2006 inventory, we found that 30 of the 31 items from the inventory were locatable, properly accounted for, and properly tagged. The Authority is in the process of developing a formalized, written, documented and approved inventory policies and procedures.

Regarding controls to ensure the continued availability of their automated systems, we determined that the Authority did not have a documented business continuity plan. Although on-site storage was being provided for the MHA's application systems, no backup copies of electronic media were being stored off-site. At the time of our audit, however, the Authority was in the process of developing off-site storage for backup media. We also determined that disaster recovery responsibilities, including LAN restoration procedures, had not been assigned nor had the Authority identified mission-critical and essential application systems and data files. We found that a criticality assessment and business impact analysis had not been formally performed. The MHA is dependent on the HAB application system to perform its mission-critical business functions and a significant disaster impacting the MHA's automated systems for an extended period would adversely impact and affect the Authority's ability to regain critical IT operations, such as processing tenant applications and accounting for rent monies and work orders.

We found that MHA did not have formal policies and procedures for the disposal of confidential records. We recommend that for guidance in developing policies the Authority refer to policy number 06-06 as promulgated by the Office of the Secretary of State regarding the disposal of confidential records.

Based upon a limited review of the Authority's primary application system, we found that the HAB system contained appropriate data fields and that data was accurate and complete for five selected records pertaining to Tenant Selection, Rental Redetermination and Site Inspection procedures, which are part of admission and continued occupancy aspects of the Federal Conventional Elderly Housing Program.

AUDIT RESULTS

Disaster Recovery and Business Continuity Planning

We determined that the Malden Housing Authority had not formulated a disaster recovery strategy or business continuity plan to outline procedures for regaining mission-critical and essential computer operations. Without a documented business continuity plan, the Authority was unable to have a tested strategy to provide reasonable assurance that processing functions rendered inoperable could be regained within an acceptable period of time. We also determined that the Authority did not have a designated alternate processing site.

The business continuity plan should address the classification of types of delays and disruptions in IT services according to impact, (e.g., catastrophic, severe, serious, or limited), processing requirements, (daily update, end-of-month processing, turnaround, reporting deadlines, minimum frequency of processing for each application and recovery times), capacity requirements for each application, written "user area" contingency plans, notification procedures, emergency drill procedures, disaster recovery test criteria, and the names, titles and contact information of key personnel assigned to recovery and security responsibilities.

Our examination of business continuity planning revealed that the Authority's management was aware of the need to have disaster recovery procedures in place and appropriate resources available to help ensure IT recovery. We acknowledge that the Authority had taken steps, such as generating daily backup copies of data files, to help ensure continuity of operations where IT systems were not damaged or inaccessible. The backup copies of electronic media stored on-site were stored in a secure manner. During our audit, the Authority was initiating corrective action to develop off-site storage of magnetic media.

A business continuity plan should consist of documented disaster recovery strategies with respect to various disaster scenarios. Without an alternate processing site, comprehensive disaster recovery strategy, or backup copies of electronic media stored in a secure off-site location, the Authority would be unable to regain IT processing capabilities within an acceptable period of time. If the LAN were damaged or destroyed, the MHA might lose mission-critical, essential, and confidential data, including tenant rental and financial information.

The objective of business continuity planning is to help ensure timely recovery of mission-critical functions should a disaster cause significant disruption to computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted business practices and industry standards for computer operations support the need for the MHA to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develop appropriate contingency and recovery plans. The MHA should assess the extent to which it is dependent upon the continued availability of information systems for all required processing or operational needs and develop its recovery plans based on the critical aspects of its information systems.

We found on-site storage of backup media to be adequately controlled and that the MHA had adequate controls over on-site computer backup media for its mission-critical software application system. We note that the MHA should implement off-site storage of backup copies of electronic media to enhance their recovery capabilities. In addition, the Authority should perform a formal risk analysis of its systems to obtain a more in-depth understanding of the impact of lost or reduced processing capabilities.

Recommendation

We strongly recommend that the Authority establish as soon as possible an adequate level of off-site storage of backup copies of electronic media. We recommend that the Authority develop a disaster recovery and business continuity plan that includes recovery strategies to address possible disaster scenarios. We also suggest that the Authority identify an alternate processing site.

We suggest that management assess the criticality of automated systems and determine time frames by which recovery of automated processing has to be achieved. Based on the results of the criticality assessment and risk analysis, the MHA should proceed with the development of a detailed, written business continuity plan for their mission-critical and essential functions.

We recommend that once the disaster recovery plan has been developed that it be tested and be subject to management review and approval. We suggest that MHA first conduct a structured walk through, or table top exercise, to review the recovery strategy and assess the level of understanding of the tasks that would need to be executed to regain processing and sustain IT operations at an alternate processing site. The plan should be tested, then periodically reviewed and updated for any changing conditions. The MHA should specify the assigned responsibilities for maintaining the plan.

Management should specify who should be trained in the implementation and execution of the disaster recovery plans under the emergency conditions outlined in the plan. The plan should identify who will perform the tasks required to fully execute the plan. Further, copies of the completed business continuity plan and user area plans should be distributed to all appropriate staff members. A copy of the plan should also be kept in a secure, off-site location.

Auditee Response

> *The MHA agrees with your Auditor's assessment that MHA controls over business continuity planning need to be strengthened in order to ensure the continued availability of automated systems. The MHA has begun the process of formulating a disaster recovery strategy that will assist in the creation of a business continuity plan. The MHA will perform both a criticality assessment and a business impact analysis in order to create LAN restoration procedures which can be administered by responsible MHA staff. The MHA will identify mission-critical and essential application systems and data files, and will perform a formal risk-analysis of MHA automated electronic systems in order to obtain a more in-depth understanding of the impact of lost or reduced processing capabilities. The MHA will provide for safe and secure off-site back-up and storage of all electronic media.*
>
> *Additionally, the MHA is in the process of creating a number of new, formal, written policies and procedures designed to assist the MHA with IT administration of inventory control, physical security, environmental controls, fixed assets IT inventory, system access security and on-site storage. Specifically, the MHA is presently working with its IT consultant, . . . in implementing the recommendations contained in the Auditor's report, and in creating the formalized written policies and technical procedures that should allow for markedly improved IT administration by the MHA, including, but not limited to, the following:*
>
> *Operational Standards and Guidelines Policies: Backup and Recovery, Business Continuity Planning, Virus Protection and Detection, Security Administration, Program Change Controls and Hardware and Software Inventory and Acquisition Policies. Each policy will include the following components: Policy Statement, Procedures and Responsibilities and General Information.*
>
> *The MHA also appreciates the Auditor's comments relative to MHA disposal of confidential records and intends to incorporate relevant suggestions into MHA's current administrative procedures.*

Auditor's Reply

We acknowledge Malden Housing Authority's goal to write a comprehensive disaster recovery strategy that will assist in the creation of a business continuity plan. In addition, we agree with the decision to develop formalized written policies and technical procedures to be incorporated in the Authority's Operational Standards and Guidelines Policies. The MHA should be aware, however, that until these goals are met and the disaster recovery and business continuity plan is tested, then the Authority remains potentially vulnerable to not being able to regain mission-critical IT processing within an acceptable period of time.