The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DeNUCCI
AUDITOR

TEL (617) 727-6200
FAX (617) 727-5891

No. 2010-1191-7T

OFFICE OF THE STATE AUDITOR'S
REPORT ON THE EXAMINATION OF
INFORMATION TECHNOLOGY–RELATED CONTROLS
AT THE
TAUNTON DISTRICT COURT

July 1, 2009 through August 18, 2010

OFFICIAL AUDIT REPORT

JANUARY 4, 2011

TABLE OF CONTENTS

INTRODUCTION

The Taunton District Court (TDC) is organized under Chapter 211B, Section 1, and Chapter 218, Section 1 of the Massachusetts General Laws. TDC's organization and management structure consists of the Judge's Lobby, Clerk-Magistrate's Office, Probation Department, and a Chief Court Officer responsible for security over the courthouse. TDC, which is located at 120 Cohannet Street, Taunton, Massachusetts, has jurisdiction for all criminal and most civil matters for the city of Taunton and the towns of Berkley, Dighton, Easton, Raynham, Rehoboth, and Seekonk.

From an information technology (IT) perspective, the Administrative Office of the Trial Court (AOTC) supports the mission and business objectives of the District Courts by managing an IT infrastructure that includes operational support of mission-critical application systems for the courts. In addition, the AOTC provides IT services, technical support, and internal control guidelines to the individual courts. The AOTC's Internal Audit Department and the Administrative Office of the District Court periodically review various processes and functions within the District Courts to help ensure compliance with applicable policies and procedures as well as providing oversight.

At the time of our audit, TDC's computer operations included 60 workstations, of which 27 were in the Probation Department, 24 in the Clerk Magistrate's Department, seven in the Judge's Lobby, and two were assigned to Court Security. The AOTC maintains the switches and hub networking equipment that provide TDC with connectivity through T1 lines allowing access to the primary computer applications administered by the AOTC. The MassCourt Lite application, which is the primary system used by TDC, is a comprehensive case management system that provides case entry, docketing, scheduling, case-related financial management, automated reports, notices and forms, and electronic storage of case documents available through the Trial Court Intranet. The MassCourt Lite system allows the District Court to manage case-related information and enable all departments and divisions to share information and monitor and track cases as they proceed through TDC's system. In addition, the Probation Department uses the Criminal Activity Record Information (CARI) system to access information on all cases involving guardianship and restraining orders and uses the BasCOT application system to record docket information for all civil cases. The Probation Department also uses the Registry of Motor Vehicles database for identification purposes. TDC relies on the Commonwealth's Information Technology Division (ITD) for access to the Massachusetts Management Accounting and Reporting System (MMARS) and the Human Resources Compensation Management System (HR/CMS). In addition, TDC uses Microsoft Office for a variety of administrative functions.

The Office of the State Auditor's follow-up audit focused on a review of certain IT-related general controls over TDC's computer operations.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed a follow-up audit of certain information technology (IT) general controls. Our audit, which was conducted from April 1, 2010 through August 18, 2010, covered the period of July 1, 2009 through August 18, 2010. The scope of the audit consisted of an evaluation of the status of prior audit results in our audit report No. 2004-1191-4T, issued December 27, 2004, regarding physical security and environmental protection for areas housing IT resources, system access security, on-site and off-site storage of backup copies of magnetic media, disaster recovery and business continuity planning, and inventory control over computer equipment.

Audit Objectives

The primary objective of our audit was to determine whether corrective action had been taken with respect to our prior audit results. Our objective regarding physical security and environmental protection controls was to determine whether adequate 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 TDC personnel had access to the automated systems used by the Taunton District Court. Furthermore, we sought to determine whether TDC, in conjunction with the AOTC, was actively monitoring password administration.

We sought to determine whether TDC, in conjunction with the AOTC, had developed a documented business continuity plan including user area plans that would provide reasonable assurance that mission-critical and essential IT-related operations could be regained within an acceptable period of time should a disaster render IT system capabilities inoperable or inaccessible. We determined whether adequate controls were in place for on-site and off-site storage of backup copies of magnetic media for the MassCourt Lite application to assist in recovery efforts.

Audit Methodology

To determine whether corrective action had been taken to address the recommendations presented in our prior audit report, No. 2004-0191-4T, we performed pre-audit work that included gaining an understanding of the TDC's mission and business objectives and reviewing prior audit workpapers and TDC's current IT environment. To obtain an understanding of the internal control environment, we reviewed the TDC's organizational structure, primary business functions, and relevant policies and

procedures, and conducted interviews with TDC management and staff. Based on our pre-audit work, we confirmed our audit scope and objectives for performing the follow-up audit.

To evaluate the IT internal control environment, we assessed the extent to which TDC had adopted AOTC's internal control policies and procedures to govern IT-related responsibilities relevant to TDC. We requested and received TDC's formal internal control guidelines that included policies and procedures contained in the Trial Court's Fiscal Systems Manual. Our audit work was focused on TDC's IT environment and did not include a review of AOTC's IT operations or facilities, except for confirming the extent to which backup copies of data files for MassCourt Lite are generated and stored off-site.

To evaluate physical security, we interviewed management and security personnel, requested written policies and procedures, and performed walk-throughs of the courthouse office areas and the telecommunication closets. We also determined who had the responsibility of providing perimeter and physical security at the courthouse. We examined the existence of controls, such as the electronic key card system, and intrusion alarms for areas housing IT resources and hardcopy files. To evaluate the controls over key card access to the courthouse, we obtained a list of personnel to whom key cards had been distributed and compared this list to a current TDC employee listing to verify that all key holders were current employees of TDC. We reviewed the levels of access privileges granted to authorized key holders and compared their level of access privileges to their job responsibilities.

To determine the adequacy of environmental protection controls, we observed the two communication closets in the courthouse and areas housing computer workstations to identify environmental protection conditions and evaluate environmental control provisions. We determined the adequacy of environmental controls over areas housing IT equipment through observations. Our examination included a review of general housekeeping; fire prevention, detection, and suppression; heat detection; uninterruptible power supply; emergency lighting; and temperature and humidity controls.

Our test of system access security included a review of procedures to authorize, activate, and deactivate access privileges to the MassCourt Lite and BasCOT applications systems used by TDC. To determine whether only authorized employees could access these systems, we obtained a system-generated list from AOTC of user accounts currently assigned to TDC employees. We compared these user lists to a current TDC employee roster to determine whether only authorized employees had access to these automated systems. We reviewed control practices regarding logon ID and password administration by evaluating the extent of documented policies and guidance provided to TDC personnel. In addition, we determined whether all employees authorized to access the automated systems were required to periodically change their passwords and assessed the frequency of password changes.

To determine whether adequate controls were in place and in effect to properly account for TDC's computer equipment, we first reviewed inventory control policies and procedures. We then obtained a current inventory list of TDC's IT resources from AOTC's inventory system of record. We determined whether the record contained appropriate data fields to identify, describe, and indicate the value, location, and condition of the computer equipment. To determine whether the inventory system of record for computer equipment for TDC was current, accurate, complete, and valid, we tested 100% of the computer equipment and determined whether there had been any equipment acquisitions or disposals during the audit period. We verified the description, location, responsible party, serial number, and inventory tag number of the computer equipment listed on the inventory record to the actual equipment on hand.

To assess the adequacy of business continuity planning, we determined whether TDC had user area plans to assist them in resuming operations should the MassCourt Lite, BasCOT, or CARI systems be inoperable or inaccessible for an extended period. We interviewed management from TDC and AOTC to determine whether a documented business continuity and disaster recovery plan was in place and had been tested, whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. We conducted a business impact analysis through interviews with management and staff to identify the potential adverse impact of an extended loss of IT capabilities.

Our audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States through the Government Accountability Office 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 version 4.1), as issued by the Information Systems Audit and Control Association, July 2007. Furthermore, we assessed TDC's compliance with the Commonwealth of Massachusetts regulations for accounting of assets as required by 802 Code of Massachusetts Regulations (CMR), as promulgated by the Comptroller. In addition, we determined whether the TDC staff was aware of and in compliance with the requirements of Chapter 647 of the Acts of 1989 for reporting missing or stolen equipment.

.

AUDIT CONCLUSION

Our review of the status of audit results from our prior audit report No. 2004-1191-4T, issued December 24, 2004, indicated that corrective action had been taken to strengthen controls regarding physical security and environmental protection, user account management, and inventory control over computer equipment. We found that the Taunton District Court's (TDC) relocation had greatly enhanced its controls over physical security and environmental controls. However, our audit revealed that control practices needed to be implemented and strengthened for disaster recovery and business continuity planning for TDC's automated systems, and password administration for the MassCourt Lite application system.

Regarding physical security over the courthouse facility, our audit revealed that TDC had controls in place and in effect to protect computer equipment from unauthorized access, use, damage, or theft. We found that TDC had physical security policies and procedures in place and that responsibilities for security were assigned. We found that TDC had video surveillance cameras, motion detectors, and security alarms in place. We determined that Court Officers were present during business hours and that all visitors, as well as packages, were subject to x-ray scanning when entering the building. In addition, we found that the use of card keys issued to TDC personnel detailing date, time, and location was maintained, monitored, and recorded by the Administrative Office of the Trial Court (AOTC). In addition, our test of key card holders determined that all issued key cards were held by current employees of the Taunton District Court. We verified that the key cards did not have TDC information, such as the name and address of TDC, printed on them.

Regarding environmental protection controls, we found that the courthouse and the two communication closets were equipped with fire prevention, detection, and suppression; heat and smoke detection; emergency lighting; temperature and humidity controls; and that the areas housing computer equipment were well organized and clean.

With respect to inventory control over computer equipment, we found that a complete and accurate list of computer equipment was being maintained. The inventory list, which assists TDC management in identifying IT resources under its control, is maintained by the AOTC to help ensure that the official system of record for property and equipment is accurate and complete for IT resources allocated to TDC. We confirmed that the TDC performed an annual physical inventory and reconciliation in April 2010 to address accounting requirements promulgated by the Office of the State Comptroller. Our audit test of the 67 computer items indicated that all items were located, properly accounted for, and tagged. The inventory records could be further enhanced by including lease cost for all computer equipment deployed.

In addition, we found that TDC had procedures in place to ensure compliance with reporting requirements of Chapter 647 of the Acts of 1989.

Regarding system access security, we found that user account management controls were in place and in effect for the MassCourt Lite and BasCOT application systems used by TDC and provided reasonable assurance that users were properly authorized to access these systems. We found that AOTC has procedures in place for the activation and deactivation of user access privileges. Our tests of user account management of the MassCourt Lite application for TDC revealed that of the 33 user accounts, all were current employees. In regards to the test of email account users, we found that all 47 users were current employees of TDC. However, our test of BasCOT users indicated that one of the 18 active user accounts was for an individual no longer employed at TDC. According to AOTC management, there was no user account activity beyond the employee's termination date.

Our audit revealed that AOTC needs to implement policies and procedures to ensure an appropriate frequency of password changes over the MassCourt Lite application system. Our audit revealed that a mandatory time frame had not been established for changing passwords and, as a result, passwords for system users had not been changed on a regular basis. In some cases, MassCourt Lite users at TDC had not changed their password since the implementation of the system in 2008. Furthermore, our audit also revealed that the requirements for password composition and length needed to be strengthened.

Regarding business continuity planning, TDC, in conjunction with AOTC, needs to further assess and develop, document, and test a comprehensive disaster recovery strategy to provide reasonable assurance that business operations could be regained in a timely manner should automated systems be rendered inoperable or compromised. We found that although the AOTC had developed a recovery strategy in the event that application systems used by the TDC should be inoperable or inaccessible, a formal, documented and tested recovery plan had not been developed. We found that TDC management was unaware of AOTC's recovery procedures for the application systems used by TDC. Furthermore, although certain procedures were in place, TDC had not documented user area and contingency plans to help ensure the resumption of business operations and activities in the event of an extended loss of IT capabilities or a major disaster or emergency.

AUDIT RESULTS

1. Password Administration

Our audit revealed that TDC, in conjunction with AOTC management, needs to implement stronger policies and procedures to ensure an appropriate frequency of password change for the MassCourt Lite application system and that the requirements for password composition and length needs to be strengthened.

Regarding our examination of password administration for the mission-critical MassCourt Lite application system, we found that management had not established a mandatory timeframe for changing passwords. Our audit indicated that many users have maintained the same password since being initially trained on the system. We found that although AOTC's security policies stated that passwords must be considered confidential and that department heads must ensure that passwords are changed periodically, password changes were not monitored or enforced. Computer industry standards recommend that organizations have documented and approved password policies that include an appropriate and enforced frequency of password changes.

Insufficient control practices over password administration places TDC at increased risk for unauthorized access to sensitive data residing on its mission-critical application. The failure to use generally accepted procedures for password composition and length places TDC at risk of unauthorized access to the MassCourt Lite application by anyone with access or the ability to gain access to the AOTC network. As a result, individuals could also gain a higher level of access privileges than they were initially authorized to have for this application system.

The policies and procedures should address authorization for system users, development of user IDs and passwords, authentication of users, establishment of audit trails, notification of changes in user status, frequency of password changes, and procedures to be followed in the event of unauthorized access or an attempt at unauthorized access.

Recommendation

We recommend that the AOTC enhance IT security policies and procedures to include more detailed requirements regarding password administration. The policies and procedures should include the length and composition of passwords (a minimum of eight alpha/numeric characters), frequency of password changes, establishment of audit trails, monitoring of required password changes, and procedures to be followed in the event of unauthorized access or when unauthorized access attempts are detected. Furthermore, we recommend that the AOTC management implement a system to prompt users to change passwords in accordance with established time frames for the MassCourt Lite application system.

Auditee's Response

We will work in conjunction with the AOTC to set up and implement guidelines to help strengthen the mandatory time frame for password changes and procedures to stop unauthorized access attempts.

2. Prior Audit Result Unresolved - Disaster Recovery and Business Continuity Planning

Our prior audit indicated that there was limited evidence that formal planning had been performed to restore TDC-based business operations in the event that automated systems and supporting technology were inoperable or inaccessible, or that operational areas within the courthouse were inaccessible.

Our current audit revealed that TDC, in conjunction with AOTC, had not developed a documented business continuity plan that would provide reasonable assurance that mission-critical data processing and business operations could be regained effectively and in a timely manner. In addition, TDC had not developed comprehensive, documented contingency plans for individual functional areas to address the potential loss of automated processing. Without contingency planning, especially including required user area plans, TDC is at risk of being unable to regain mission-critical business operations within an acceptable period of time. An extended loss of processing capabilities could adversely affect TDC's ability to perform its primary business functions and could result in significant delays in processing caseloads.

We found that TDC had not documented responsibilities to develop and maintain detailed continuity plans to guide user areas in the event that automated systems were inoperable or inaccessible for an extended period of time. Although TDC was able to articulate the procedures needed to be performed under various disaster scenarios to regain business functions, none of these strategies has been formally documented or tested. For example, Court management indicated that court business could be conducted at another district court; however, a detailed strategy to regain operations has not been documented or tested. TDC also needs to identify the nature and extent of court or business activities that could be conducted in the absence of AOTC-supported systems and/or in the event of damage or inaccessibility to TDC's facilities.

According to TDC management, under a disaster scenario in which TDC could not conduct business on a short-term basis, TDC's operations could be relocated to an alternate district court where access to the MassCourt Lite application system could be provided. TDC could then be able to schedule hearings and use MassCourt Lite for docketing and data input. It is our understanding that on a long-term basis, the AOTC's centralized Information Technology Department could provide IT resources to support TDC's operations at another court facility. Regarding backup files, AOTC confirmed that backup copies of data files for the MassCourt Lite application are generated and electronically vaulted at an off-site location.

Effective disaster recovery and business continuity plans should provide specific instructions for various courses of action to address different types of disaster scenarios. The plans should identify how, by whom, and when mission-critical and essential services will be provided given the loss of existing IT capabilities. The business continuity plan would detail the manner and order in which operations would be restored, identify the policies and procedures to be followed, and detail recovery tasks and responsibilities.

The viability of the business continuity planning process requires continued management commitment. Senior management and system users should be closely involved in business continuity planning to help ensure that there is a clear understanding of the entity's information system environment, that determinations of system criticality and the risks and exposures associated with the systems are correct, that appropriate IT and user area plans are developed based on the relative criticality and importance of systems, and that adequate resources are available.

Generally accepted practices and industry standards for computer operations support the need for organizations to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans, if required. Therefore, TDC should assess the extent to which it is dependent upon AOTC for all required IT-enabled processing or IT capabilities, and perform, in conjunction with AOTC, a risk analysis of IT systems to gain a better understanding of associated risks and the impact of lost or reduced processing capabilities. The risk analysis should identify the relevant threats that could render the IT infrastructure inoperative, the cost of recovering the systems, and the likelihood of threats and disaster scenarios and the potential frequency of occurrence. Recovery and contingency plans should then be developed based on mission-critical and essential operational requirements.

Recommendation

We recommend that TDC, in conjunction with the AOTC, develop a documented business continuity plan, including detailed user area plans specific to TDC's operations. We recommend that the business continuity plan document TDC's strategy for conducting business at other court locations. An assessment of criticality and business impact should be performed at least annually, or upon major changes to TDC operations or the IT environment. Moreover, TDC should obtain an adequate level of understanding and assurance as to the disaster recovery strategies that will be implemented by AOTC should IT capabilities need to be restored. TDC should identify required time periods by which IT capabilities need to be recovered to support TDC's mission-critical and essential business functions.

The business continuity and contingency plan, including user area plans, should document TDC's recovery and contingency strategies with respect to various disaster scenarios. The recovery plan should contain all pertinent information, including clear assignment of key personnel and their roles and

responsibilities needed to efficiently recover mission-critical and essential operations within the respective time frames. We recommend that the business continuity plan be tested and periodically reviewed and updated, as needed, to ensure its viability. The completed plan should be distributed to all appropriate staff members who must be trained in the execution of the plan under emergency conditions. We also recommend that TDC request input, instructions, and guidelines from AOTC to ensure continuity of IT and business operations should the applications used by TDC become inoperable or inaccessible.

Auditee's Response

> *We will work in conjunction with the AOTC to set up and implement guidelines to ensure continuity of IT and business operations should the Court become inoperable or inaccessible due to an unforeseen disaster.*

Auditor's Reply

We acknowledge TDC's intent to address business continuity planning. TDC's business continuity plan should provide sufficient detail regarding different recovery strategies, including relocation to another court facility, and that associated tasks and responsibilities be clearly defined. Furthermore, we strongly suggest that recovery and business continuity plans be reviewed, tested to the extent possible, and updated as operational requirements or risk factors dictate. We will review this area during future audits.

2. Prior Audit Results Resolved

a. Physical Security and Environmental Protection

Our prior audit determined that physical security and environmental protection controls needed to be strengthened at TDC. The audit conclusions presented in our prior audit report were based on the TDC's former court location in 2004.

Our follow-up review noted that TDC has relocated to another facility that provides improved controls regarding physical security and environmental protection for its operations. Our current examination of physical security and environmental protection controls over the courthouse revealed that TDC had controls in place and in effect to protect IT-related assets from unauthorized access, use, damage, or theft in the areas housing the IT equipment. We also found that IT equipment was properly safeguarded against fire, heat, and water damage, and that adequate housekeeping was in effect.

b. Inventory Control over Computer Equipment

Our prior audit indicated that inventory control of IT-related equipment needed to be strengthened to provide reasonable assurance that TDC's IT-related assets were properly recorded and accounted for and safeguarded against unauthorized use, theft, or damage. Specifically, we found that the AOTC's master inventory and TDC's inventory lists of IT resources were not in agreement and that inventory records had not been reconciled.

Our current audit confirmed that TDC, in conjunction with AOTC, had strengthened inventory controls over IT equipment. We found that a complete and accurate list of computer equipment was being maintained by AOTC and TDC. The inventory list, which assists management in identifying IT resources under its control, is maintained by the AOTC to help ensure that the official system of record for property and equipment is accurate and complete for IT resources allocated to TDC. We confirmed that the TDC had performed a physical inventory and reconciliation to address accounting requirements promulgated by the Office of the State Comptroller.

c. User Account Management

Our prior audit revealed that access privileges to TDC's application systems were not being deactivated in a timely manner. Our audit test revealed that 18 out of the 61 user accounts were associated with individuals who were no longer employed at TDC.

Regarding our current audit, we found that user account management controls were in place and in effect for the application systems utilized by TDC and provided reasonable assurance that users were properly authorized to access the systems. Our audit found that all active user accounts were for current employees, except for one user account that had not had any associated activity since the individual had left the employment of TDC. We found that there were procedures in effect for the activation and deactivation of user access privileges. Our tests of user account management of the MassCourt Lite application revealed that of the 33 user accounts, all were current employees of the TDC. In regards to the test of email account users, we found that all 47 users were also current employees of TDC. Our test of BasCOT users indicated that of the 18 user accounts, one user was no longer a TDC employee and our audit tests confirmed that the account had no activity since the employee terminated employment at TDC.