A. JOSEPH DeNUCCI
AUDITOR

# The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

**NO. 2003-1173-4T**

## OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE CENTRAL BERKSHIRE DISTRICT COURT PITTSFIELD DIVISION

**July 1, 2002 through July 31, 2003**

**OFFICIAL AUDIT REPORT**
**FEBRUARY 19, 2004**

TABLE OF CONTENTS

## INTRODUCTION

The Central Berkshire District Court, Pittsfield Division is organized under Chapter 211, Section B and Chapter 218, Section 1 of the Massachusetts General Laws. The Court's organizational management structure consists of the Judge's Lobby, Clerk-Magistrate's Office, and the Probation Department. The Court has jurisdiction over all criminal, civil and juvenile matters within Central Berkshire County consisting of the City of Pittsfield and the towns of Becket, Dalton, Hancock, Hinsdale, Lanesboro, Lenox, Peru, Richmond, Washington, and Windsor. For the 2003 fiscal year, the Court received $1,269,393 of state funds and had processed revenue of approximately $380,000 from sources, such as cash bail receipts, fines, fees, and penalties.

Chapter 478 of the Acts of 1978 reorganized the courts into seven Trial Court departments, including the District Court. Since the implementation of Chapter 478, the central administrative office has been referred to as the Administrative Office of the Trial Court (AOTC). From an information technology perspective, the AOTC supports the mission and business objectives of the District Courts by administering the IT infrastructure, including mission-critical applications installed on file servers located at the AOTC's Information Technology Department in Cambridge. In addition, the AOTC provides IT services and technical support to individual courts and maintains master inventory records for the courts under its jurisdiction.

The primary IT functions at the Central Berkshire District Court are supported and maintained by AOTC and the Office of the Commissioner of Probation. At the time of the audit, the Court's computer operations were supported by 21 microcomputer workstations; eleven in the Clerk-Magistrate's Office, seven in the Probation Department, and three in the Judge's Lobby. The workstations were connected to four routers linked through T1 lines and connected to AOTC's wide-area network (WAN). The primary applications operating on the AOTC file servers that are accessible through the Court's workstations included the Basic Court Operation Tools (BasCOT), Warrant Management System (WMS), the Probation Receipt Accounting System (PRA), and the Criminal Activity Record Information System (CARI). The Clerk-Magistrate's Office utilizes the BasCOT to record docket information and the WMS to track outstanding warrant information issued from all courts under the jurisdiction of the AOTC. The Probation Department utilizes the CARI application system to track dispositions from courts regarding criminal and juvenile offenses, as well as restraining orders and the PRA application system is used to account for functions related to receipt and disbursement of bail, fines, fees, and penalties.

The Office of the State Auditor's examination focused on a review of selected IT-related general controls over the Court's IT environment.

## AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

### Audit Scope

We performed an information technology (IT) related audit at the Central Berkshire District Court, Pittsfield Division from April 23, 2003 to July 31, 2003 covering the period July 1, 2002 through July 31, 2003. The scope of our audit included an evaluation of IT-related controls pertaining to IT organization and management, physical security, environmental protection, inventory control of IT resources, and business continuity planning.

### Audit Objectives

Our primary audit objective was to determine whether adequate controls were in place and in effect for selected functions in the IT processing environment. We sought to determine whether the Court's IT-related internal control framework, including policies, procedures, and practices, provided reasonable assurance that IT-related control objectives regarding physical security, environmental protection, inventory control and availability of systems 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 computer equipment and associated IT resources.

We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that the Court's IT resources were properly accounted for. In addition, we determined whether the Court had a business continuity strategy, including user area plans in place to assist them in regaining business operations supported by technology within an acceptable period should a disaster render computerized functions inoperable or inaccessible.

### Audit Methodology

To determine the audit scope and objectives, 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 management to gain an understanding of the Court's operations and IT control environment. To obtain an understanding of the Court's activities and internal control environment, we reviewed the organizational structure and primary business functions. We assessed the strengths and weaknesses of the internal control system for selected activities and, upon completion of our pre-audit work, determined the scope and objectives of the audit.

Regarding our review of IT-related management control practices, we interviewed court management, reviewed documentation, and assessed relevant IT-related internal controls. Our review work was limited to relevant IT-related policies and procedures within the Court's facility.

To evaluate physical security, we interviewed court management and security personnel, inspected physical access controls, and reviewed procedures to document and address security violations and/or incidents. Through observation and examination of security controls, we determined the adequacy of physical security controls over areas housing IT equipment. We examined controls such as security devices, office door locks, metal detectors, and intrusion alarms.

To determine the adequacy of environmental controls, we conducted a walk-through and determined the extent to which environmental protection controls were in place for the telecommunication closet and areas housing microcomputer workstations. We assessed the sufficiency of control-related procedures and practices 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 and water detection; uninterruptible power supply; emergency lighting and shutdown procedures; and humidity control and air conditioning. Audit evidence was obtained through interviews, observation, and documentation reviews.

To determine whether adequate controls were in place and in effect to properly account for IT-resources located at the Court, we reviewed inventory control policies and procedures and requested a copy of the Court's inventory of IT resources and AOTC's system of record for the Court's IT resources. Even though we did request the Court's inventory control records for IT-related assets, we considered the AOTC's master inventory as the official system of record because the AOTC was responsible for maintaining fixed asset inventory records and promulgating policies and procedures for all courts. We also determined whether the Court's inventory control records for IT resources were being updated annually and could be reconciled to the AOTC's inventory system of record.

To assess the adequacy of business continuity planning, we evaluated the extent to which the Court had user area plans that could be activated in conjunction with AOTC's disaster recovery plans to resume IT operations should mission-critical and essential application systems be rendered inoperable or inaccessible. We determined whether the Court was aware of AOTC's business continuity plans and efforts to resume IT operations should the application or communication systems be rendered inoperable. We interviewed senior management to determine whether the Court in conjunction with AOTC had determined the criticality of application systems, and the associated risks and exposures to computer operations. In addition, we determined whether AOTC was storing backup copies of computer-related media in an off-site location through interviews with our Office's audit staff conducting an IT audit at the AOTC.

Our audit was conducted in accordance with generally accepted industry standards.

## AUDIT CONCLUSION

Our audit disclosed that although the Court had certain IT-related controls in place, controls pertaining to physical security, environmental protection, inventory control over IT-related resources, and business continuity planning needed to be strengthened. In addition, we found that there was a general absence of documented policies and procedures to address IT-related functions performed at the Court.

Our examination of the Court's organization and management revealed that there was an established chain of command. Our review of IT-related activities disclosed that the primary IT functions were supported and maintained by the AOTC's IT Department. Due to the nature and limited extent of the IT environment at the Court there was no established IT department. Although the Court had limited controls in place over IT activities, we found that there were no available IT-related policies and procedures to guide Court personnel.

Regarding physical security, the Court did have certain security controls in place such as the presence of security officers and hand-held metal detectors used to screen persons and personal items through the public entrance during normal business hours. We observed that courthouse doors other than the main entrance were kept locked and were equipped with security alarms. In addition, we found only Court employees were allowed access to restricted areas and were required to wear ID badges. However, our audit revealed that Court's telecommunications room was not in a secure area of the facility and that adequate controls were not in place to prevent or detect unauthorized access at various access points in the court. We found that certain areas had no intrusion alarms in place.

We found that controls related to environmental protection at the courthouse and, in particular, the telecommunications room needed to be strengthened. We found that there were no smoke, heat, or water detection devices in the telecommunications room that houses the routers that connect the Court to AOTC's file servers. In addition, there were no provisions for an emergency generator in the event of a temporary or extended loss of electrical power. We found that the dedicated HVAC unit in the telecommunications room was in non-working condition. We also found that general housekeeping in the telecommunications room needed to be strengthened. Further, from a personnel safety perspective, we observed that there was no public address system in place to facilitate an evacuation of the building in the event of an emergency.

Our review of the Court's inventory control procedures revealed that adequate procedures were not in place to provide reasonable assurance that IT-related resources were properly accounted for. We determined that the Court did not maintain a perpetual IT fixed-asset inventory as required by AOTC's "Fiscal Systems Manual." We also determined that the Court did not perform an annual physical inventory of IT related items and therefore we could not compare AOTC's master listing of inventory to any records maintained by the Court. In addition, fixed-asset cost data, acquisition dates, and receiving

documentation were unavailable. The Court, in conjunction with the AOTC, should establish a perpetual inventory record that should be periodically reconciled to the AOTC's master inventory record that must contain appropriate data elements, including cost data, acquisition dates, and references to receiving documentation.

At the time of our audit, the Court did not have business continuity, or user plans, to address the loss of automated processing should IT systems be inoperable. The Court was also unaware of the general adequacy of any business continuity plans or strategies to be exercised by AOTC. In addition, we found that the Court, in conjunction with the AOTC, had not performed a criticality assessment of application systems and their associated risks. The Court needs to address the risks of not being able to rely upon the continued availability of AOTC-based systems, access to AOTC systems, or the loss of critical IT resources at the Court and to develop, in conjunction with AOTC, appropriate continuity or contingency plans.

## AUDIT RESULTS

1. IT-Related Organization and Management

Although the Court had certain IT-related general controls in place, control practices would be strengthened by having documented IT-related policies and procedures readily available to guide staff in performing IT tasks and activities. Since IT operations were supported by centralized AOTC-based systems, the extent of required documentation for IT-related functions performed at the Court should be developed in conjunction with the AOTC's IT Department. Documented IT-related policies and procedures for physical security, environmental protection, business continuity planning, access security, and inventory control of IT resources would strengthen overall IT control practices. Although certain controls were in place with regard to these functions, having written policies and procedures would help ensure that operational and control objectives would be met for the security and accounting of IT resources and, to the extent possible, availability of processing functions.

Formal documentation of IT-related policies and procedures provides a sound basis for helping to ensure that desired actions are taken and that controls are exercised and monitored to meet control objectives and prevent or detect and address undesired events in a timely manner. Formal documentation also enables personnel to attain a more in-depth understanding of their responsibilities and duties and improve their level of competence and performance. In addition to outlining responsibilities and task requirements for IT-related activities, procedures should be in place to provide reasonable assurance that control practices are working as intended. Chapter 647 of the Acts of 1989 requires all state agencies to document and approve internal control policies and procedures as part of a system of generally accepted control practices.

In the absence of documented policies and procedures, employees may rely on individual interpretations of what is required or how to best manage and control IT-related systems and resources. In such circumstances, inconsistencies or omissions may result, and key control objectives may not be adequately addressed. Furthermore, a lack of documented policies and procedures undermines management's ability to monitor and evaluate the performance of IT-related activities and functions. As a result, management may not be sufficiently assured that desired actions will be taken.

Recommendation:

We recommend that the Court, in conjunction with AOTC, formulate and adopt appropriate IT-related policies and procedures to provide sufficient, formal guidance for IT-related tasks and activities. Control practices would be strengthened by having written IT- related policies and procedures regarding physical security, environmental protection, access security, business continuity planning, and inventory control of IT resources.

Auditee's Response

> *Please be advised that I look forward to developing with AOTC appropriate policies and procedures.*

Auditor's Reply

Documented controls, policies, and procedures provide a framework to guide and direct staff in the discharge of their responsibilities. It is our hope that the development of documented policies and procedures for the Court's IT environment will be accomplished before the implementation of the new MassCourts application system.

2. Physical Security and Environmental Protection

Our audit disclosed that the Court had certain physical security controls in place to safeguard IT-related resources. We found that upon entering the courthouse, all visitors passing through the main entrance were required to enter through a metal detector, and all packages had to be scanned through an X-ray machine. We also observed that only Court staff occupied areas where the microcomputer workstations were located and that public access to those areas was prohibited. However, certain physical security controls needed to be strengthened to prevent or detect unauthorized physical access in certain areas. We found that physical security needed to be strengthened by having appropriate barriers and intrusion alarms installed at various points where unauthorized access could be gained. We also found that the telecommunication closet was not located in a secure area of the Court facility.

Our review confirmed that there were certain environmental protection controls in place such as an emergency evacuation plan for the entire building, an emergency shut off valve for water lines for the entire building, air conditioning for areas housing microcomputer workstations, and functional fire extinguishers on each floor in the courthouse. However, we determined that environmental protection controls needed to be enhanced with respect to emergency lighting and the installation of heat, smoke, humidity, and water detectors in the communications room. We also observed that the telecommunications room was not subject to ventilation or air conditioning. We also found that general housekeeping in the telecommunications room needed to be strengthened as evidenced by the presence of papers, excess dust, and boxes.

Generally accepted computer industry practices indicate the need for appropriate physical security and environmental protection controls to be in place to ensure that the IT resources are properly safeguarded and protected. An annual risk analysis should include an assessment of risks and vulnerabilities of IT resource security, integrity and availability.

The Court should adopt appropriate physical security and environmental protection policies and procedures to ensure that IT resources located throughout the Court are protected from unauthorized

access, use, damage or theft. In addition, the IT resources also need to be properly safeguarded against loss or damage due to excessive heat, water, humidity or fire. Furthermore, inadequate physical security and environmental protection controls over the telecommunications room increases the risk that the Court could be unable to access critical information should connections to the WMS, PRA and CARI application systems be disrupted or disabled.

Recommendation:

We recommend that the Court, in conjunction with AOTC, develop and maintain IT policies and procedures for physical security and environmental protection for all areas housing IT resources and equipment. We recommend that windows where access could be gained be equipped with intrusion alarms or motion detectors and, if warranted, protected with bars or other barriers. We also recommend that the Court consider the installation of smoke, heat, humidity and water detectors in the telecommunications room. Further, we recommend that the Court evaluate the need for intrusion alarms or motion detectors for windows where unauthorized access could be gained.

Auditee's Response

> *I look forward to the implementation of IT policies and procedures for the physical security and environmental protection of IT resources and equipment. I trust there will be money authorized and allocated to implement your recommendations.*

Auditor's Reply

We acknowledge that the courthouse facility requires funds to be properly maintained and physically secure. We recommend that requests for assistance to the AOTC be made in writing. In addition, management should consider, upon consulting with AOTC's IT Department, to either relocate the telecommunication room or strengthen environmental protection controls over the existing room. We reiterate our recommendation that the Court evaluate the need to install intrusion alarms or motion detectors for windows where unauthorized access could be gained.

3. Business Continuity Planning

Our audit revealed that the Court, in conjunction with the AOTC, had not collaborated to develop a formal business continuity strategy, including user area plans, that would provide reasonable assurance that critical data processing operations could be regained effectively and in a timely manner should a disaster render systems inoperable or inaccessible. Furthermore, the Court had not assessed the relative criticality of the automated systems supporting Court operations and identified the extent of potential risks and exposures to business operations. Although the AOTC generated backup copies of magnetic media for the business functions processed through AOTC's file servers, our audit revealed that the

Court, in conjunction with AOTC, had not developed user area contingency plans to address a potential loss of automated processing. Without adequate disaster recovery and contingency planning, including required user area plans, the Court was at risk of not being able to perform certain functions should their automated systems be disrupted or lost. A loss of processing capabilities could result in significant delays in processing caseloads.

The environmental deficiencies existing at the Courthouse place even more emphasis on the need to develop a detailed business continuity plan should mission-critical application systems become unavailable for an extended period of time. Without a comprehensive, formal, and tested recovery and contingency strategy, including user area plans, the Court's ability to access information related to the WMS operating on the AOTC's file servers, and the CARI and PRA systems operated by the Commissioner of Probation would be impeded. Without access to these applications, the Court would be hindered from obtaining information regarding outstanding warrant information, or unable to confirm that fines, fees, and penalties were being collected by the Probation Department. Furthermore, the Court would be unable to access all trial court dispositions regarding criminal cases. The absence of a comprehensive recovery strategy could seriously affect the Court's ability to regain critical and important data processing functions.

An effective disaster recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios. The plan should identify the policies and procedures to be followed, detailing the logical order for restoring critical data processing functions, either at the original site or at an alternate-processing site. For user environments, appropriate user area plans outlining recovery or contingency steps should be in place. The user area plans should be coordinated with overall enterprise-based business continuity plans.

The success of the business continuity planning process requires 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 and their platforms 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. The Court, in conjunction with the AOTC, should perform a risk analysis of the systems and identify the impact of lost or reduced processing capabilities.

Generally accepted practices and industry standards for computer operations support the need for each entity 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, the entity should assess the extent to which it is dependent upon the continued availability of information systems for all required processing or operational needs and should develop its recovery plans based on the critical aspects of its information systems.

We believe that AOTC and Court management have not emphasized the importance of developing business continuity and contingency plans along with user area plans to address the loss of automated systems for an extended period of time.

Recommendation:

We recommend that the Court assess the relative criticality of their automated processing and develop and test in conjunction with AOTC appropriate user area plans to address business continuity. We recommend that an assessment of criticality and business impact be performed at least annually, or upon major changes to Court operations or the IT environment.

The business continuity plan, or user area plan, should document the Court's recovery and contingency strategies with respect to various disaster scenarios and outline any necessary contingencies. The recovery plan should contain all pertinent information needed to effectively and efficiently recover critical operations within the needed time frames. We recommend that business continuity and user area plans be tested, and periodically reviewed and updated, as needed, to ensure their viability. The completed plans should be distributed to all appropriate staff members who must be trained in the execution of the plan under emergency conditions.

Auditee's Response

> *I look forward to developing, in conjunction with AOTC, appropriate procedures and policies to effectuate your recommendations.*

Auditor's Reply

We acknowledge that the Court is aware of the need for business continuity planning for its mission-critical and essential applications. At a minimum, we recommend that user area plans and procedures be established to address business continuity planning, and that the plans be periodically reviewed and updated as necessary. This is especially critical in the future as the Court increases its reliance on information technology in performing its primary business functions.