The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

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

A. JOSEPH DeNUCCI
AUDITOR

NO. 2003-0290-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE REGISTRY OF VITAL RECORDS AND STATISTICS

JULY 1, 2002 TO NOVEMBER 11, 2003

OFFICIAL AUDIT REPORT

JUNE 25, 2004

TABLE OF CONTENTS

INTRODUCTION

The Registry of Vital Records and Statistics (RVRS) was established under the Secretary of State's Office in 1841 and is the oldest statewide records retention system in the nation. On January 1, 1977, the Division of Vital Statistics was transferred from the Office of the Secretary of State to the Department of Public Health (DPH), and a Registrar for the agency was appointed subject to the approval of the Public Health Council. Per Massachusetts General Law (MGL) Chapter 46, Section 17, the Registry's mission is to collect, process, correct, maintain and issue copies of records and vital statistics that occur in the Commonwealth of Massachusetts. The Registry of Vital Records and Statistics is responsible for the legal registration, collection, and reporting of almost 250,000 births, deaths, marriages, and divorces annually. Because of the sensitive nature of some of the information maintained, the Registry is bound under the privacy acts of confidentiality, MGL Chapter 111m, Sections 24A and B and Chapter 46, Sections 2A and 13.

The Registry, which is located at 150 Mount Vernon Street in Dorchester, operates as a division of the Department of Public Health, where it collects and maintains an archive of vital records and statistics occurring within the Commonwealth of Massachusetts. RVRS retrieves and certifies copies of vital records and statistics directly to the public or through a web-based program called Vital Chek. In addition, the Registry has contracts with government agencies (for example, National Center for Health Statistics, Social Security Administration) and other entities for retrieving and certifying certificates.

At the time of our audit, the agency's information technology consisted of sixty microcomputer workstations configured in a Windows NT 4 local area network (LAN). The LAN's file servers, which were dedicated to the agency's IT operations, were housed in the RVRS Dorchester office. The agency is further connected through a file server at DPH for access to the Commonwealth's wide area network (WAN). The Registry uses FoxPro to support its database applications and SQL Server for programming development under a contract with Science Applications International Corporation (SAIC). At the time of our audit, there were 716 separate Fox Pro databases with data stored Fox Pro, Access, mainframe sequential files, mainframe VSAM files, and mainframe Adabas. IT staffing at the Registry consisted of two full-time RVRS employees and one contracted employee.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

We performed an information technology (IT) audit at the Registry of Vital Records and Statistics for the period of July 1, 2002 through November 11, 2003. The audit, which was conducted from April 7, 2003 to November 11, 2003, consisted of an examination of IT-related internal controls pertaining to organization and management, physical security and environmental protection for computer equipment, system access security, hardware and software inventory, business continuity planning, and on-site and off-site storage of backup copies of magnetic media. We also reviewed data input and output processing activities that were standard for the FoxPro databases. We reviewed policies and procedures pertaining to research services and providing certificates through the Public Access Counter. In addition, we reviewed the receipts process for these services. We also reviewed the adequacy of internal control documentation for the Public Access Counter and IT-related functions for compliance with MGL Chapter 647 of the Acts of 1989 and for internal control monitoring.

Audit Objectives

The primary objective of the audit was to determine whether adequate controls were in place to provide reasonable assurance that IT-related resources would be safeguarded and available when required.

With respect to IT-related controls, we sought to determine whether adequate IT organization and management controls were in effect to properly support the Registry's IT processing environment. We sought to determine whether adequate controls regarding physical security and environmental protection were in place and in effect to safeguard computer operations and IT resources, except for backup copies of media stored off site. A further objective was to determine whether adequate controls were in place and effect to prevent and detect unauthorized access to application systems and data files available through the agency's networked microcomputer workstations. Our objective with respect to hardware and software inventory was to determine whether IT resources were properly identified, recorded, and accounted for in the Registry's inventory records.

We sought to determine whether the Registry's business continuity plan would provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period of time should a disaster render computer systems inoperable or inaccessible. In conjunction with reviewing business continuity planning, we sought to determine whether proper backup procedures were being performed and whether copies of backup magnetic media were being stored in secure on-site and off-site locations.

With respect to data input integrity for the agency's information systems, we sought to determine whether adequate input and output controls were in place and whether the systems were subject to appropriate access security controls.

With respect to internal control documentation, we sought to determine whether the RVRS, acting under the auspices of the Department of Public Health, had an agency-specific internal control plan and whether documented internal controls were sufficiently comprehensive and detailed to support agency business functions, including IT operations. In addition, we sought to determine whether appropriate mechanisms were in place to monitor and evaluate the effectiveness of the agency's system of internal controls.

Audit Methodology

To determine the audit scope and objectives, we performed a pre-audit survey regarding the Registry's mission, business objectives, business processes and IT environment. The pre-audit work included interviews with senior management; a review of policies, procedures, and other internal control documentation; conducting a high-level risk analysis; and observation of IT-related areas. We assessed the strengths and weaknesses of the internal control system for selected IT-related activities. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

To obtain an understanding and evaluate the organization and management of IT operations, we reviewed the Registry's organizational structure with respect to IT operations and evaluated reporting lines, job descriptions, oversight mechanisms, and separation of duties. We reviewed IT policies and procedures to determine the level of documentation regarding the IT general control areas related to our audit.

To determine whether IT-related assets were adequately safeguarded, we reviewed physical security and environmental protection over computer equipment and backup copies of magnetic media in on-site storage through observation, conducting interviews with RVRS management and staff, and by completing appropriate audit checklists.

We reviewed the Registry's logical access security policies and procedures to prevent and detect unauthorized access to the LAN, applications, and data files and connectivity to Commonwealth's WAN (MAGNet). We reviewed the access privileges of staff who had been authorized to access the Registry's IT systems and applications residing on ITD's mainframe. We determined whether system users who were authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes. Further, to determine whether users were restricted to only the application programs and data files to which they had been authorized, we reviewed a scan of software available on end-user desktops and compared access privileges on a sample of desktops. We further reviewed access privileges and related controls with the Registry's Director of Systems and Development. To determine whether adequate controls were in place to ensure that access privileges to the automated systems were granted to only authorized agency users, we compared the list of individuals authorized to access RVRS's IT systems to the list of current RVRS employees.

To determine whether the Registry's hardware inventory record was current, accurate, complete, and valid, we reviewed information on purchased items and compared it to the information recorded on the inventory record, and conducted verification tests of IT assets between the inventory record and the items on hand. We traced sixty one hardware items (100%) to the inventory record and vice versa to determine whether the hardware items were physically locatable, properly tagged, and properly recorded and accounted for with their historical cost. Further, to test whether purchased hardware items were being listed on the inventory record and could be physically located at the Registry, we compared purchase orders and invoices to the inventory record and to actual equipment purchased by the RVRS during fiscal year 2003. We compared the state tag identification numbers listed on the hardware inventory record to the actual tag numbers on the equipment on hand.

To determine whether the appropriate controls were in place to ensure that only authorized copies of software were installed on the automated systems, we reviewed related policies and procedures for the acquisition, installation and monitoring of the use of software. We interviewed the MIS Director regarding the policies and procedures and obtained a current list of software designated by the agency for authorized use. Our examination included obtaining a scan of the LAN to validate the existence of only authorized software. Using the Random Number Generator (RNG) in Microsoft Excel, we then tested 8 of 43 workstations (approximately 20%) to validate the scan. In addition, to test whether unauthorized software could be installed, we attempted to install an unauthorized program with the permission of the Director of Systems and Development. To determine whether the RVRS had implemented adequate controls to account for licensed copies of application software residing on its file servers and microcomputer workstation, we first sought to obtain an inventory list of software installed or available for use. We then reviewed the software inventory list.

To assess the adequacy of business continuity planning, we reviewed the nature and extent of formal planning for the resumption of computer operations in the event that IT systems were inoperable or inaccessible. We interviewed RVRS management to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been evaluated, and whether a written business continuity plan was in place. We reviewed policies and procedures regarding the generation and storage of backup copies of magnetic media. We determined whether appropriate controls were in place to ensure that backup copies of data files and software would be available should the automated systems be rendered inoperable. Our review of backup procedures included an evaluation of provisions for on-site and off-site storage of critical backup tapes. We also interviewed RVRS management responsible for generating backup copies of computer-related media. We reviewed procedures for generating, inventorying and storing backup copies of magnetic media. Our review did not include a review of the off-site location.

To determine whether adequate internal control documentation was in place and to assess its appropriateness, we interviewed senior management at RVRS and reviewed existing policy and procedure documentation and IT-related audit trails. We also requested documentary evidence of internal control monitoring activities to determine whether appropriate mechanisms were in place to monitor and evaluate the effectiveness of RVRS's system of internal controls. In this regard, we reviewed internal control requirements as established by Chapter 647 and the Office of the State Comptroller's Internal Control Guidelines.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) for the United States and generally accepted industry practices. With respect to IT-related control objectives and controls, we used the Information Systems Audit and Control Association's and the IT Governance Institute's Control Objectives for Information and Related Technology (CobiT), published in July 2000, to identify IT management control practices as criteria for review.

AUDIT CONCLUSION

We found that adequate controls were in place at the Registry of Vital Records and Statistics to provide reasonable assurance that IT-related control objectives would be met with respect to IT organization and management, physical security, environmental protection, software inventory, and system access security for the local area network environment and related workstations. Although certain IT-related controls and policies and procedures were in place, internal control documentation and monitoring and evaluation needed to be strengthened. While efforts had been taken to address hardware inventory control, further improvement was needed to provide increased assurance that asset protection objectives would be addressed. Although the Registry's business continuity plan appeared to be adequate, recovery strategies needed to be formally reviewed and tested in conjunction with the Department of Public Health.

Our review of the Registry's IT-related organization and management indicated that adequate organizational controls were in place and that IT-related policies and procedures were well documented. Although RVRS, in conjunction with DPH, appeared to have adequate control procedures in place to maintain vital statistics and process revenue from researching and providing copies of licenses, the Registry did not have an internal control officer or an internal control plan. In addition, we found that the DPH internal control plan did not adequately address operations or IT functions specific to the Registry. Based on the internal control documentation reviewed, IT-related controls examined, and interviews, sufficient evidence was not provided to demonstrate an adequate level of internal control monitoring and evaluation.

We determined that physical security controls in place at the RVRS office provided reasonable assurance that IT-related resources would be safeguarded from unauthorized access through the use of security guards and appropriate security devices for office entrances and areas housing IT resources.

With respect to environmental protection, we found adequate controls to be in effect to provide reasonable assurance that IT operations were functioning in a proper environment to safeguard computer equipment and other IT-related assets as well as agency personnel and the general public. These controls included the computer room having smoke and fire detectors, a fire alarm system, handheld dry chemical fire extinguishers, an automatic fire suppression system, and a self-contained air filter/dehumidifier and air conditioning unit. In addition, all computer equipment was raised a minimum of 8 to 10 inches off the floor to protect against damage from minimal flooding.

Regarding system access security, we found that documented policies of logical access controls provided reasonable assurance that only authorized users had access to the RVRS's computer system on which the Registry's application systems reside. We found that controls over the administration of user IDs and passwords provided reasonable assurance that access privileges would be deactivated or appropriately modified should RVRS employees terminate employment or incur a change in job requirements. During our audit, nothing came to our attention to indicate that access privileges granted to individuals were inappropriate given their job responsibilities.

Although the Registry maintained an inventory record of computer hardware and software and was conducting periodic physical inventories, controls needed to be strengthened to ensure that all relevant information was recorded. We found that the inventory record did not include the attributes of cost, date of purchase, and equipment serial numbers for individual items. Our tests did confirm that hardware items listed on the inventory record were locatable, tagged, and could be accounted for. We also found that purchased software products were accounted for and verifiable in accordance with licensing agreements. In addition, controls were in place to restrict the installation of unauthorized software.

With respect to business continuity planning, we found that RVRS had a documented business continuity strategy and disaster recovery plan. We recommend that the business continuity plan be tested and formally approved to ensure that the recovery strategies provide reasonable assurance that mission-critical and essential data processing operations for administrative and user functions could be regained effectively and in a timely manner should a disaster render automated systems inoperable.

AUDIT RESULTS

1. INTERNAL CONTROL DOCUMENTATION, MONITORING, AND EVALUATION

Our review of RVRS's internal control documentation revealed that although the Registry had documented internal control policies and procedures and a DPH-designated internal control plan, RVRS could not provide an agency-specific internal control plan that detailed internal controls in place for its administration and business operations. Although RVRS did maintain policies and various sets of operating procedures to cover its business functions, the policies and procedures were not assimilated into a formally-documented, comprehensive agency-specific internal control plan.

Our review of the DPH internal control plan indicated that it did not specifically address operations and IT functions performed at the Registry. In order to comply with Chapter 647 of the Acts of 1989, an Act Relative to Improving Internal Controls Within State Agencies, the Registry needs to develop its own internal control plan that addresses RVRS' operations. Without an adequate internal control plan, the Registry cannot be adequately assured that it has an appropriate system of internal control, that assets are safeguarded, and that operational effectiveness and efficiency is promoted. The internal control plan should also describe the accounting system and other information systems, identify control and monitoring activities, and indicate that an entity-wide risk assessment was performed.

Chapter 647 of the Acts of 1989 requires "internal control systems of the agency are to be clearly documented and readily available for examination. Objectives for each of these standards are to be identified or developed for each agency activity and are to be logical, applicable, and complete. Documentation of the agency's internal control systems should include (1) internal control procedures, (2) internal control accountability systems, and (3) identification of the operating cycles. Documentation of the agency's internal control systems should appear in management directives, administrative policy, and accounting policies, procedures and manuals." Given the extent to which technology is used to support the Registry's operations, IT functions should be addressed by the internal control system and documented, or referenced, in the internal control plan.

Based on our review of internal control documentation, there was little documented evidence that RVRS performed comprehensive monitoring and evaluation of controls related to the areas covered in this audit. Monitoring and assurance mechanisms should be in place to determine whether internal controls are operating as intended to meet established operational and control objectives. We found that the Registry maintained only a limited monitoring or internal control function occurring through informal meetings of IT personnel. Without the diligence of the MIS staff, the Registry would be at increased risk of damage or loss of information systems should a disaster occur.

While the Registry was responsible for the development and exercise of an appropriate internal control structure, including internal control documentation, to provide reasonable assurance that operational and control objectives would be addressed, we found that an internal control officer had not been appointed for RVRS to monitor and evaluate controls. Due to the increase in operational activity through the Internet by way of the Vital-Chek System, the increase of fees (over $1.5 million estimated) and the increasing reliance of information technology in the recording and compilation of statistics, greater emphasis on improving IT-related internal control documentation and monitoring is warranted. In particular, to strengthen the overall framework of control, risk analysis should be performed and control metrics should be established for each business activity. In addition, RVRS should be responsible for documenting its own monitoring and evaluation activities to ensure that appropriate internal controls are in place and in effect to meet operational and control objectives.

There are various sources that RVRS can reference to assist in developing control self-assessment and monitoring and evaluation techniques, such as the "Internal Control Guides" from the Office of the State Comptroller and the "Internal Control – Integrated Framework" document from the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.

In the absence of a detailed internal control plan and control monitoring and evaluation, the Registry cannot be adequately assured that IT-related control policies and procedures are consistently implemented and applied. We believe that the volume of processing of various business activities through RVRS warrants the implementation of a formal monitoring and evaluation process.

Recommendation:

The RVRS, in conjunction with DPH, should strengthen its internal control documentation by developing a comprehensive and cohesive agency-specific internal control plan. We recommend that RVRS establish a framework for its internal control plan to which existing sets of internal documentation can be included or cross-referenced. The internal control plan should include administrative, accounting and operational control procedures including IT functions performed by RVRS.

We recommend that RVRS also strengthen its internal control practices by performing risk analysis on a periodic basis sufficient to identify business and operational risks that need to be addressed by internal controls. We recommend that RVRS, in conjunction with DPH, establish appropriate mechanisms to monitor and evaluate the effectiveness of internal controls. The latter would include mechanisms to measure whether controls are operating as intended and developing control self-assessment processes where appropriate. The RVRS, in conjunction with DPH, should define and document the responsibilities of an internal control officer as required by the Office of the State Comptroller.

Auditee's Response

> *Of the first finding concerning strengthening of RVRS internal control documentation with DPH:*
>
> - *RVRS will work with DPH finance to develop an agency specific internal control document as recommended.*
> - *An individual will be assigned to be the local internal control officer and work with DPH finance to define and document his/her responsibilities.*

Auditor's Reply

We believe that RVRS will be able to strengthen internal control by addressing control objectives and respective controls in conjunction with DPH. Having DPH work with RVRS on internal control allows DPH to establish an internal control framework within which all DPH agencies can manage. We support the assignment of a local control officer to coordinate internal control initiatives and monitoring with DPH.

2. HARDWARE INVENTORY

At the time of our audit, we found that IT-related fixed-asset controls needed to be strengthened to provide for the proper accounting of the RVRS's inventory record. Our audit review of the RVRS master inventory record for hardware items revealed that recorded IT-related equipment at the

RVRS was validated for all the items as to location and proper identification tagging. However, although RVRS had an appointed inventory officer, the inventory system of record did not include the attributes of cost, date of purchase, and equipment serial numbers for individual items.

Because of insufficient documentation on IT procurements or shipments of equipment received, we were unable to determine inventory information related to purchase date and cost. The absence of readily available packing slips or lists of equipment serial numbers tied to individual procurements inhibited our ability to confirm that all equipment purchased was properly recorded and available for use. If the equipment record were incomplete and items not listed were lost or misplaced, then the inventory record would not assist management in helping to detect missing items. Access to supporting documentation regarding equipment acquisitions and installations is valuable to management's efforts to verify the inventory system of record. We were unable to identify the cost and date of purchase for specific items because either the purchase orders were unavailable or did not contain an attached packing list for bulk purchases. Without appropriate documentation, we were unable to trace the items purchased from their respective purchase orders to the inventory system of record. In addition, we were unable to obtain an annual master inventory list of the prior fiscal year to be able to reconcile the list from one fiscal year to the next.

Regarding authorized software, we found that the Registry had established a list of software authorized for installation and that certain controls were in place to restrict unauthorized software installation. To test whether unauthorized software could be installed, we attempted, with the permission of the network administrator, to install an unauthorized program, and were appropriately refused by the operating system, since the attempted installation conflicted with the proper permissions set by the network administrator.

Generally accepted industry standards and sound management practices indicate that adequate controls be implemented to account for and safeguard property and equipment. In addition, Chapter 647 of the Acts of 1989, states, in part, that "…the agency shall be responsible for maintaining accountability for the custody and use of resources and [shall] assign qualified individuals for that purpose, and [that] periodic comparison should be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts."

Shortcomings in inventory control were the result of insufficient attention and less than adequate assignment of inventory control responsibilities. The absence of a more-detailed and complete inventory record may hinder RVRS 's ability to manage IT resources, detect theft and unauthorized use of IT resources, and assess future technology and IT configuration requirements.

Recommendation:

We recommend that RVRS management, in conjunction with DPH, strengthen inventory control policies and procedures for RVRS. We recommend that the inventory system of record include data fields for cost, date of purchase, and equipment serial numbers. In addition, to support IT configuration management, we recommend that the inventory record include the status of the IT resource in terms of usability and business continuity requirements. We further recommend that documentation of annual inventory procedures be strengthened.

Auditee's Response:

On adding tracking information to the RVRS IT inventory:

- *The inventory officer will add to the current inventory columns to track purchase order numbers, cost, date of purchase, and an indicator if the item is active or is surplus. Serial numbers are currently part of the inventory.*
- *At the end of each fiscal year the inventory will be archived in order to provide year to year comparisons.*
- *In addition, RVRS will work with DPH finance to merge the RVRS IT inventory with a DPH central inventory system that will also contain necessary tracking information.*

Auditor's Reply:

We are pleased that RVRS management is addressing our recommendations regarding inventory control over IT-related resources. With respect to data fields within inventory control records in the current inventory, archiving of the inventory at the end of each fiscal year, and merging the RVRS IT inventory with a DPH central inventory system, we acknowledge that addressing these issues should improve overall inventory control.