The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DE NUCCI
AUDITOR

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

NO. 2009-0290-7T

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, 2007 through August 31, 2009

OFFICIAL AUDIT REPORT

FEBRUARY 3, 2010

TABLE OF CONTENTS

INTRODUCTION

The Registry of Vital Records and Statistics (RVRS) was established under the Office of the Secretary of State 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. According to Chapter 46, Section 17, of the Massachusetts General Laws, the RVRS's mission is to collect, process, maintain, and issue copies of records and vital statistics. 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. In addition, the RVRS has contracts with government agencies (e.g., National Center for Health Statistics, Social Security Administration) and other entities for retrieving and certifying certificates.

The RVRS's mission is supported through the use of three network servers connecting 60 workstations at the main office in Dorchester. The RVRS utilizes an additional server for access to the DPH mainframe, allowing connectivity to the Commonwealth's wide area network (WAN). At the beginning of our audit, the Systems and Development Unit (SDU) was responsible for managing the RVRS's information technology requirements and consisted of two staff members based at the RVRS. In accordance with Section 2 of Executive Order No. 510, "Enhancing the Efficiency and Effectiveness of the Executive Department's Information Technology Systems," the IT staff were re-assigned to the Executive Office of Health and Human Services and were no longer part of RVRS.

The primary software application, referred to as the Divisional Application System, that is used by RVRS is a FoxPro application operating in a Microsoft Windows environment. The Divisional Application System stores, prints, and queries data pertaining to birth, death, marriage, divorce, and legal name-change information. The application tracks vital record information that has been transferred via mail from the city and town clerks. The RVRS also relies on a web-based program, VitalChek, which allows the public to order copies of Massachusetts vital records including birth, death, marriage, and divorce records.

The RVRS relies on the Commonwealth's Information Technology Division (ITD) for access to the Massachusetts Management and Accounting and Reporting System (MMARS) and the Human Resources Compensation Management System (HR/CMS).

The Office of the State Auditor's examination was limited to a review of certain IT general controls over and within the RVRS's information technology environment.

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 controls at the Registry of Vital Records and Statistics (RVRS). Our audit, which was conducted from March 23, 2009 through August 31, 2009, covered the period of July 1, 2007 through August 31, 2009. Our audit included an examination of system access security controls, business continuity planning, and on-site and off-site storage of backup copies of magnetic media at RVRS. We also reviewed the status of audit results in our prior IT Audit Report, No. 2003-0290-4T, issued June 25, 2004, regarding internal control documentation and inventory control over computer equipment.

Audit Objectives

Our primary audit objective was to determine whether the RVRS's IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that IT-related control objectives would be met to support business functions. A further objective was to assess the status of prior audit results and determine whether corrective action had been taken to address audit results and recommendations made in our prior Audit Report, 2003-0290-4T. We sought to determine whether appropriate corrective action had been taken to strengthen and develop internal control documentation and to implement inventory controls to provide reasonable assurance that computer equipment would be properly recorded and accounted for and safeguarded against unauthorized use, theft, or damage.

Our objective regarding system access security was to determine whether adequate controls were in place to provide reasonable assurance that only authorized personnel had access to the RVRS's automated systems and that password administration was appropriately monitored by RVRS management. Further, we determined whether adequate disaster recovery and business continuity plans were in place to provide reasonable assurance that mission-critical operations could be regained within an acceptable period of time should a disaster render IT functions inoperable or inaccessible. We determined whether adequate procedures for on-site and off-site storage of backup media to support system and data recovery operations were in place and in effect.

Audit Methodology

To evaluate whether corrective action was taken on our recommendations presented in our prior Audit Report, No. 2003-0290-4T, we performed pre-audit work that included a review of prior audit work

papers and gaining an understanding of the RVRS's current IT environment. We reviewed our prior recommendations regarding documented IT policies and procedures, inventory control over computer equipment, system access security, business continuity planning, and on-site and off-site storage of backup media.

Regarding our review of IT-related policies and procedures, we interviewed senior management at both RVRS and at the Department of Public Health (DPH). We reviewed and assessed relevant internal control documentation and reviewed the organizational structure and reporting lines of the RVRS. We determined whether policies and procedures were in place and in effect, and whether they provide guidance to RVRS staff. We identified which IT activities were being performed at RVRS and determined whether there were documented policies and procedures to cover those activities.

Our tests of system security included a review of procedures used to authorize, activate, and deactivate access privileges for both the RVRS network and for certain applications residing on the DPH network. To determine whether only authorized employees were accessing the automated systems, we obtained system-generated user lists from both RVRS and DPH for individuals granted access privileges to the automated systems and compared the lists to an RVRS personnel listing, dated May 1, 2009. We interviewed RVRS personnel regarding the frequency of password changes and reviewed control practices regarding logon ID and password composition and administration. We examined whether all individuals authorized to access system applications were required to change their passwords periodically and to determine the frequency of the changes.

In order to verify that all users of the RVRS network were current employees, we obtained a system-generated user account list containing 141 user accounts as of July 9, 2009. We compared the user account list to a current RVRS employee roster. We developed an exception list of those individuals no longer requiring access privileges to the RVRS network and reviewed the exception list with RVRS management. We performed an additional test of access privileges granted to RVRS employees for certain applications residing on the DPH network. We obtained a system-generated user list from DPH containing 61 RVRS user accounts. In order to verify that all user account holders were current RVRS employees, we compared this list to an official employee roster, dated May 1, 2009. Our audit did not include an examination of controls over network security.

To assess the adequacy of inventory control procedures for computer equipment, we conducted an examination of the RVRS inventory to determine whether appropriate controls were in place and in effect to properly account for and safeguard IT resources. We examined policies and procedures regarding fixed-asset inventory to determine whether the RVRS was in compliance with the Office of the State Comptroller's regulations regarding fixed-asset control. We conducted a test of the 129 items

listed on the RVRS inventory, dated March 1, 2009. We examined the inventory record for identification tag numbers, locations, descriptions, and historical costs.

To assess the adequacy of business continuity planning, we interviewed RVRS and DPH management to determine the responsibility for various systems utilized at RVRS. Although systems reside with DPH, ITD, and the RVRS, our audit focused on the application systems at RVRS. We determined whether any formal planning had been performed to resume computer operations should the Divisional Applications System operated by RVRS be rendered inoperable or inaccessible. In addition, we determined whether the criticality of the Divisional Applications System had been assessed, and whether risks and exposures had been evaluated. In addition, to evaluate the adequacy of internal controls for the protection of data files though the creation and storage of backup media and hardcopy files, we interviewed RVRS staff, examined the on-site storage locations, and determined whether off-site storage was being provided.

Our audit was conducted in accordance with generally accepted government auditing standards (GAGAS) of the United States and generally accepted industry practices. Audit criteria used 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, 2007.

AUDIT CONCLUSION

Based on our audit at the Registry of Vital Records and Statistics (RVRS), we found that certain internal controls were in place for IT-related functions and that IT-related control objectives would be met regarding inventory control for computer equipment and the generation and on-site storage of backup computer media for application systems operated by RVRS. However, we found that controls needed to be implemented or strengthened for IT-related policies and procedures, including an internal control plan for RVRS functions, user account management, password administration, and business continuity planning. We found that policies and procedures relating to IT activities needed to be formally documented and that appropriate business continuity or contingency plans needed to be developed in conjunction with the Department of Public Health (DPH). In addition, we found that RVRS had stopped providing off-site storage of backup copies of data files for its mission-critical Divisional Application System residing on a file server located at the RVRS.

Our review of IT-related activities disclosed that although the primary oversight for IT functions at RVRS resided with the Department of Public Health's IT Department, we found that the DPH internal control plan did not adequately address operations or IT functions specific to RVRS. As a result of the general absence of agency-specific documented IT policies and procedures, sufficient guidance over the IT functions at RVRS was not being provided. Critical control activities, including user account management, password administration, and off-site storage of backup media, were not being sufficiently monitored.

Our review of system security disclosed that controls for RVRS access to the DPH network were adequate. Our audit test revealed that all RVRS user accounts were authorized and current. However, our examination of the Divisional Application System revealed that access controls needed to be strengthened. We found that 89 user accounts had not been deactivated for individuals no longer employed or authorized by RVRS. Our audit disclosed that RVRS was unable to provide information relating to when these accounts should have been eliminated and as a result RVRS was unable to identify when the user accounts should have been deactivated. We recommend that the RVRS immediately review access privileges to its automated systems and eliminate all unauthorized user accounts. In addition, formal policies and procedures need to be developed between DPH's Human Resources Department and the RVRS. A documented procedure should be in place for communicating any changes in user status that could warrant modification or deactivation of user accounts. Regarding password administration over the Divisional Application System, we found that employees were not required to change passwords on a predefined basis and that users were required to use personal

information in their user IDs. We found no evidence of documented policies and procedures regarding password composition and frequency of change.

With respect to inventory control of computer equipment, our prior Audit Report, No. 2003-0290-4T, indicated that the inventory records did not include the attributes of cost, date of purchase, and equipment serial numbers for individual items. Our current audit confirmed that RVRS added the data fields in the inventory master file, but had not entered any of the specific data. In addition, we found that RVRS was adhering to the regulations promulgated by the Office of the State Comptroller requiring that annual physical inventories be performed.

We found that controls over business continuity planning and off-site storage of backup computer media needed to be strengthened. Our audit disclosed that a formal, tested disaster recovery and business continuity plan was not in place. We recommend that the RVRS, in conjunction with DPH, test its business continuity plan to assess its viability and establish a process for routinely updating the plan based on changes to the technology, business processes, or staffing. The RVRS should ensure that all personnel responsible for business continuity tasks and activities be clearly identified and adequately trained.

We found that the RVRS lacked adequate controls over off-site storage of backup copies of systems and data files. Our audit revealed that, contrary to sound business practices, RVRS had terminated the practice of exchanging weekly backup media with DPH's Cancer Registry and, as result, had no off-site backup of mission-critical information in electronic form. We recommend that RVRS management either resume the media exchange with the Cancer Registry or find a secure off-site location to store its backup media.

AUDIT RESULTS

1. IT-Related Policies and Procedures

Although our audit revealed that RVRS had extensive policies and procedures in place to provide guidance and standard operating procedures for its business processes, there was a general lack of IT policies and documented procedures to address IT functions or activities. We found that management control practices needed to be documented to ensure that the staff members have sufficient guidance for performing IT-related functions. At the time of our audit, the RVRS did not have documented and approved policies and procedures in place to adequately address IT functions and to help provide reasonable assurance that control and business objectives would be achieved for system access security, inventory control of computer equipment, off-site storage of backup copies of magnetic media, and business continuity planning.

Chapter 647 of the Acts of 1989 states that "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 RVRS's operations, IT functions should be addressed by the internal control system and documented in the internal control plan.

In order to comply with Chapter 647 of the Acts of 1989, the RVRS, in conjunction with DPH, needs to develop its own agency-specific internal control plan. Without an adequate internal control plan, the RVRS cannot be assured that an appropriate internal control system, including policies, procedures, practices and organizational controls, is in place and is monitored and evaluated to assess its effectiveness. The internal control plan and formal documentation of IT-related policies and procedures helps ensure that control objectives are met, assets are safeguarded, and that operational effectiveness and efficiency is promoted. The absence of formal policies and standards may lead employees to rely on individual interpretations of what is required to be performed. As a result, management may not be adequately assured that desired actions will be taken.

Our audit revealed that although a security control officer had been appointed per our prior recommendation, it appeared that only minimal communication had been made with DPH in the development of specific policies and procedures to address IT activities at RVRS.

The absence of documented IT-related policies and procedures and an internal control plan undermines management's ability to provide adequate guidance to staff, ensure that appropriate controls are in place, and that internal controls are monitored and evaluated.

Recommendation

We recommend that RVRS, in conjunction with DPH, develop a comprehensive internal control plan specific to RVRS. The RVRS should establish a framework for its internal control plan so that internal control policies, procedures, and practices specific to the RVRS can be included or cross-referenced. As such, the internal control plan would address IT-related functions performed by RVRS staff. We further recommend that management develop and document procedures to ensure appropriate monitoring and evaluation of the adequacy and effectiveness of documented IT internal control systems. We recommend that RVRS solicit the assistance of DPH and centralized IT services to identify existing IT policies and standards that should be adopted for IT-related activities and identify any policies and procedures that need to be developed or documented.

Auditee's Response

The results of the audit found that while RVRS had extensive policies and procedures in place to provide guidance for their business processes, RVRS needs to customize policies and procedures to address RVRS-specific IT functions or activities. Global IT policies and procedures also need to be better communicated and monitored within DPH and personnel trained. RVRS has since worked together with key Department of Public Health (DPH) staff to assess the findings, develop strategies for addressing the findings and to develop a response.

The Registry of Vital Records and Statistics (RVRS) is a division within the Bureau of Health Information, Statistics, Research, and Evaluation (BHISRE) within the Department of Public Health (DPH). Following the audit recommendation RVRS has solicited the assistance of DPH and centralized Information Technology resources to respond to the findings. RVRS is working with the DPH Information Security Officer (DPH ISO), in developing RVRS-specific sections of DPH plans for IT-related policies and procedures.

The DPH has created an Information Security Program (ISP), as per Executive Order 504 (EO504), which contains a listing of all the critical RVRS applications that contain personally identifiable information and lists them along with their compliance drivers in a separate Electronic Security Plan (ESP). In addition to this RVRS will solicit the assistance of IT resources available to DPH and centralized EOHHS services to identify existing IT policies and standards that should be adopted for RVRS IT-related activities and identify any policies and procedures that need to be improved, developed or documented. This process will ensure that the internal control

plan addresses controls for all RVRS databases, including those with and without personally identifiable data. This ISP/ESP combination, together with information in other DPH internal control documents forms the basis of the RVRS Internal Control Plan. RVRS will supplement this with RVRS-specific administrative and operational procedures that together will comprise the RVRS Internal Control Plan following the DPH-suggested format for internal control documents.

The DPH Privacy Office liaison at RVRS performed the EO504 Self Audit Questionnaire (SAQ) for RVRS critical applications in August and September of 2009. In our preliminary review the SAQ covers all essential topics that would be contained within an RVRS-specific Internal Control Plan, including password policy and internal control procedures. We are in the process of filling in gaps as necessary. The SAQ for RVRS (citing all major applications) was completed in a fashion consistent with the method being used throughout DPH and submitted to the Information Technology Division (ITD) by September 18, 2009 after the audit window closed. Based on the findings from this questionnaire, recommendations will be made regarding the development of additional policies and training to enhance the protection of personally identifiable information at the RVRS.

Regarding communication between DPH and RVRS of password policy (and all others that cover DPH data including all located within RVRS), a project to provide a DPH Information Security Policy Book has been created and a beta version has been shared with IT staff assigned to RVRS and RVRS management; it will become available during 2010 for DPH-wide user access.

To further communicate this new password policy and DPH Policy Book to RVRS staff, the DPH ISO conducted an Encryption Workshop at RVRS on November 23, 2009. The workshop reviewed all major relevant policies that cover RVRS, where copies of these policies can be found, and describes scenarios where further protection of personally identifiable information requires approved encryption technology.

Further, all RVRS (and DPH) employees are required to take the mandatory EO504 online (or paper-based) training as soon as possible which outlines the DPH Information Security Program, and which includes among the many statutes relevant to DPH, those which specifically apply to RVRS.

While considerable progress has already been made, RVRS will continue to work with available IT and DPH resources to comply with all recommendations contained in the audit

Auditor's Reply

We commend the RVRS for its work with DPH to formally document IT policies and procedures to address its IT environment. Documentation of policies and procedures is an essential component of an internal control structure, along with documentation of business processes and supporting systems and the record of activity for each system. However, once a comprehensive and cohesive internal control plan for the RVRS is developed, it is essential to implement monitoring and evaluating mechanisms to

ensure that internal control policies and practices are in effect to provide reasonable assurance that operational and control objectives will be met.

2. User Account Management and Password Administration

Our audit revealed that controls need to be strengthened to ensure that only authorized users have access to the Divisional Application System. We found that appropriate policies and procedures regarding deactivation of user access accounts and privileges were not documented and that there was no evidence that user account activity was being monitored and evaluated. Regarding password administration, we found that controls needed to be strengthened over password composition and that the frequency of change of passwords was informal and undocumented.

Although we found that adequate controls were in place to authorize and activate user accounts for the RVRS network, controls needed to be strengthened to ensure timely deactivation of access privileges for users no longer authorized to access the automated systems. Our tests of system access security for the Divisional Application System indicated that 89 of 141 user accounts had not been deactivated for individuals who were no longer employed by the RVRS. Moreover, our audit revealed that formal policies and procedures had not been in place that require notification from DPH's Human Resources Department to the Systems and Development Unit or security administrator to initiate the removal of access privileges of individuals whose employment had been terminated with the RVRS. The RVRS was unable to provide information regarding user identity, date of termination of employment, and the date of last account activity. Our audit evidence indicated that a reconciliation of the user account list to authorized employees was not being performed on a periodic basis for the RVRS's application systems. Our audit test of RVRS user accounts to the DPH network indicated that all user accounts reconciled to a list of authorized user accounts.

Our audit revealed that increased monitoring of user accounts was required to evaluate user account access and identify user accounts that should be deactivated. The failure to deactivate or delete user accounts in a timely manner places automated systems at risk of unauthorized access or having an individual gain higher access privileges than currently authorized. We also found that the application system or the system upon which it resides does not have the ability to detect or record unauthorized logon or data-change activities. As a result, certain information residing on the Divisional Application System could be been vulnerable to unauthorized access.

The Control Objectives for Information and Related Technology (CobiT), issued by the Information Systems Audit and Control Association, is a generally applicable and accepted standard for IT security and control that provides a control framework for management, business process owners, and IT functions. Additional controls recommended by the CobiT control framework include having

procedures to ensure timely action for requesting, activating, suspending, and closing user accounts; having a control process to periodically review and confirm access rights; and regularly performing scheduled comparisons of resources with recorded accountability to help reduce the risk of errors, fraud, misuse, or unauthorized change.

Regarding our examination of password administration for the mission-critical Divisional 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. Regarding our examination of password controls over access to the DPH network, we found that although DPH had documented policies for password administration, passwords were not being changed in accordance with either the Commonwealth's Information Technology Division's standards or the Office of the State Comptroller's Internal Control Guide for Departments.

The Internal Control Guide for Departments states, in part, "an employee's password should be changed or deleted immediately upon notice of his/her termination, transfer, or change in responsibility." CobiT's control practices recommend that organizations have password policies that include "an appropriate and enforced frequency of password changes." In addition, computer industry standards advocate that policies and procedures for all aspects of system access security be documented and approved to provide a basis for IT systems and data. 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 an unauthorized access attempt or unauthorized access.

Recommendation

We recommend that RVRS and DPH perform an immediate review of the status of all active users to the Divisional Application System and deactivate privileges for those individuals who no longer require access. We recommend that management develop written policies and procedures requiring timely notification to the security administrator of any of changes in employee status that could warrant change or deactivation of access privileges to the RVRS network or application systems. We also recommend that the RVRS implement preventive and detective control mechanisms, such as vigilant monitoring of access accounts to ensure that only authorized individuals have appropriate levels of access to IT resources.

Subsequent to the audit period, when we brought this issue to management's attention, DPH's Office of Information Security issued a new DPH password policy entitled "Password Policy/Access Control" on

October 7, 2009 that directed all DPH employees to increase system access security for all DPH facility IT systems.

Auditee's Response

Department of Public Health (DPH) Information Technology Services (ITS) has introduced new standards for password composition and is addressing the issue of changing passwords. The Registry of Vital Records and Statistics (RVRS) is working with ITS to develop new procedures for authorizing and activating user accounts for the RVRS network. RVRS is developing a system to ensure deactivation for users no longer authorized to access the automated systems and to regularly monitor user accounts.

The Divisional Applications are aging legacy FoxPro applications. IT personnel assigned to RVRS do not recommend changing the password data file to add or remove user profiles. It would be necessary to procure the services of a FoxPro specialist programmer each time a change is necessary since the add/remove function does not already exist. So instead, the corrective action is to archive the file and create a new file reflecting the current users.

In addition, a formal procedure for notifying IT managers of staff reorganization that may affect user accounts, roles and rights is being developed DPH-wide and will therefore apply to RVRS as well. RVRS will continue to work with available IT and DPH resources to comply with all recommendations contained in the audit.

The DPH password policy gap which surfaced during the audit and also as part of the EO504 SAQ process was addressed when the DPH ISO, provided RVRS IT with a new Password and Access Control policy on October 9, 2009 followed by an updated version on November 18, 2009. Derived from ITD's password policy, it states that user passwords must meet minimum complexity standards and be changed every 42 days. Further, this same policy applies to passwords guarding access to applications. This policy has been implemented DPH-wide, including newer applications at RVRS.

However, due to software constraints, the RVRS Divisional Applications can only accommodate password lengths up to 5 characters. This set of applications will be gradually replaced by the new Vitals Information Processing (VIP) system, the first module of which will be rolled out in the latter half of calendar year 2010. This VIP system will have EOHHS Virtual Gateway access control and application role-based security.

Auditor's Reply

We acknowledge the RVRS's action for addressing the security concerns related to user account management. We believe that efforts to improve communication regarding changes in network security status or access privileges for employees will enhance user account management. We commend DPH and the RVRS for initiating steps to address the security concerns related to user account management. Further, assurance mechanisms, such as timely reconciliation of user accounts to currently authorized users, should be exercised to ensure that only authorized users have access, user privileges are clearly

specified for active user accounts, and that user accounts for network and application system access are monitored and evaluated.

3. Business Continuity Planning and Off-Site Storage of Backup Media

Our audit revealed that although RVRS had a designated alternate processing site located at a DPH facility and had developed a documented business continuity plan, key elements of the plan had not been updated since it was initially drafted in 2003. We found that emergency contact information was outdated and key personnel listed in the plan were no longer employed at the RVRS. Our analysis indicated that the plan lacked sufficient detail for restoring critical functions in the event that automated systems were rendered inoperable or inaccessible. We also determined that off-site storage of the weekly backup tapes for the mission-critical Divisional Application System had been discontinued, further jeopardizing recovery efforts.

To ensure that a formal business continuity plan is documented and available, the RVRS should document recovery strategies with respect to various disaster scenarios. The lack of a detailed, tested plan to address the resumption of processing capabilities may hinder the recovery of essential and confidential data should a disaster render IT systems inoperable. Without a formal, tested recovery strategy, RVRS may experience difficulties in fulfilling its mission of collecting, preserving, and reporting permanent vital records in an efficient and effective manner.

Business continuity planning helps ensure timely recovery of mission-critical functions should a disaster cause significant disruption to computer operations. Generally accepted business practices and industry standards for computer operations support the need for the RVRS to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops and maintains appropriate contingency and recovery plans. The RVRS should perform a risk analysis of the systems and clearly understand the impact of lost or reduced processing capabilities.

Although we found on-site storage of backup media to be adequately controlled, our audit revealed that the RVRS was not providing for off-site storage of its mission critical applications. We found that since a management change in the Systems Unit, the RVRS has discontinued its policy and practice of exchanging backup tapes with another DPH agency, the Cancer Registry. As a result of failing to provide off-site storage, there is no assurance that the back-up media would be readily available to assist recovery efforts.

Recommendation

We recommend that RVRS management establish a framework of procedures to ensure that the criticality of all automated systems is evaluated and that business continuity planning is assessed for all system applications. We recommend that RVRS, in conjunction with the Department of Public Health, review the information technology environment and perform a criticality assessment and risk analysis of all automated systems. Based on the results of the assessment, RVRS should proceed with revising and updating a business continuity plan.

Once the plan has been revised, it should be tested, then periodically reviewed and updated for any changing conditions. The RVRS should specify the assigned responsibilities for maintaining the plan and for supervising the implementation of the tasks documented in the plan. Management should specify who should be trained in the implementation and execution of the plans under all emergency conditions and who will perform each required task to fully implement the plans. Further, copies of the completed business continuity 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.

Regarding the off-site storage of computer media backup, we recommend that RVRS management re-establish its practice of providing a weekly off-site backup of all automated systems.

Auditee's Response

The Registry of Vital Records and Statistics (RVRS) is a division within the Bureau of Health Information, Statistics, Research, and Evaluation (BHISRE) within the Department of Public Health (DPH). Contact information has been updated in the Continuity of Operation Plan for BHISRE, including RVRS. RVRS will work with the management of BHISRE and DPH to review the information technology environment and perform a criticality assessment and risk analysis of all automated systems. Based on the result of this assessment, RVRS will work with BHISRE and DPH to revise and update the Continuity of Operation Plan (COOP).

Once the plan has been revised, it will be tested, periodically reviewed and updated. Responsibilities will be assigned and staff trained. Copies will be distributed to appropriate staff and a copy of the plan will be kept in an off-site location.

IT staff assigned to RVRS have worked with the DPH IT Help Desk to develop a plan for weekly off-site encrypted backup of all automated systems.

RVRS will continue to work with available IT and DPH resources to comply with all recommendations contained in the audit.

Auditor's Reply

We acknowledge RVRS's action in having appropriate back-up procedures to aid recovery efforts. The planned development of a comprehensive and well-documented business continuity and contingency strategy is essential to ensure timely recovery of mission-critical and essential business functions and systems.

4. Status of Prior Audit Results

a. Prior Audit Results Unresolved-Internal Control Documentation, Monitoring, and Evaluation

Our prior audit found that DPH's internal control plan did not adequately address operations or IT functions specific to the RVRS. 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.

Our current audit determined that management control practices still need to be documented to ensure that RVRS staff have sufficient guidance for performing IT-related functions.

We recommend that RVRS, in conjunction with DPH, develop a comprehensive internal control plan specific to RVRS. The RVRS should establish a framework for its internal control plan so that internal documentation can be included or cross-referenced. The internal control plan should include administrative and operational control procedures, including IT functions performed by RVRS.

b. Prior Audit Results Resolved-Inventory Control over Computer Equipment

Our prior audit found that although the RVRS 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.

We found that RVRS was adhering to the regulations promulgated by Office of the State Comptroller requiring that annual physical inventories be performed**.** Although our current audit confirmed that RVRS had added the recommended data fields in the inventory master file or store, we recommend that the RVRS enter the required data for these fields