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. 2008-0242-4T

OFFICE OF THE STATE AUDITOR'S
REPORT ON THE EXAMINATION OF
INFORMATION TECHNOLOGY-RELATED CONTROLS AT
THE DEPARTMENT OF MENTAL HEALTH
METRO BOSTON AREA OFFICE

July 1, 2004 through April 29, 2008

OFFICIAL AUDIT REPORT
DECEMBER 23, 2008

TABLE OF CONTENTS

INTRODUCTION

The Department of Mental Health (DMH), which is organized under Section 1, Chapter 19 of the Massachusetts General Laws, as amended, is comprised of a central administrative office in Boston, six area offices, three state mental health hospitals, eight mental health centers and 28 local service delivery sites located throughout the Commonwealth. The DMH also provides inpatient care at two state public health hospitals, the Tewksbury State Hospital and the Lemuel Shattuck Hospital, which are operated by the Department of Public Health. Each Metro Boston Area (MBA) mental health center provides either inpatient and/or outpatient services. In addition, DMH hires and trains police personnel who provide security at MBA mental health centers. The DMH and its organizational units are placed under the purview of the Executive Office of Health and Human Services.

The Metro Boston Area is comprised of the MBAO, three mental health centers, and four site offices in Boston and Cambridge, as well as inpatient units at the Lemuel Shattuck Hospital. The Metro Boston Area serves the cities of Boston, Cambridge, Chelsea, Revere, Somerville and the towns of Brookline and Winthrop.

The Metro Boston Area Office (hereinafter referred to as the MBAO) is one of six area offices within the Massachusetts Department of Mental Health. MBAO's administrative office is located in the building that houses the Dr. Solomon Carter Fuller Mental Health Center in Boston. At the time of our audit, the MBAO was staffed by an Area Director, two Deputy Directors, a Medical Director, and 62 employees.

The primary mission of the MBA's mental health centers is to provide comprehensive mental health and support services to meet the needs of clients requiring care for mental illness. Metro Boston Area mental health centers provide emergency evaluation and assessment, short term and long-term inpatient and/or outpatient care, including forensic evaluations required by Massachusetts' courts and rehabilitative and support services in a community setting. According to the MBAO, during fiscal year 2007 the Metro Boston Area's mental health centers had the capacity to provide services for 185 inpatients (125 adults at Lemuel Shattuck Hospital and 60 adults at Erich Lindemann Mental Health Center) and 1,135 outpatients at the Massachusetts Mental Health Center. The Lemuel Shattuck Hospital's inpatient units provide care and treatment for patients with serious mental disorders.

The Metro Boston Area received a total allocation of Commonwealth funds from DMH for fiscal year 2007 of $127.8 million. In addition, MBAO received a total of $5.9 million in client services revenue from third-party payers and $23.7 million in revenue from DMH billings on behalf of MBAO.

MBAO's computer operations at the Dr. Solomon Carter Fuller Mental Health Center were supported by 11 file servers and 205 workstations installed throughout the administrative office that were configured in a local area network (LAN). The file servers were connected to a wide area network (WAN) to the Commonwealth's Information Technology Division's mainframe that provides access to the Massachusetts Management Accounting and Reporting System (MMARS), Human Resources Compensation Management System (HR/CMS), and other network services, including e-mail. In addition to the workstations available for MBAO personnel, the Office had six notebook computers that were assigned to senior managers. Overall, IT operations and services supporting the MBAO were provided by DMH's Applied Information Technology Division.

The primary application used by MBAO to support its mission-critical business functions is the vendor-developed Mental Health Information System (MHIS). MHIS provides automated processing for a variety of important client-related services, including admissions, medical records management, coding diagnosis, therapeutic information, billing and accounts receivable, and accounts payable. MHIS is also used to monitor in-patient and outpatient medications. The MHIS application is supported through a cluster of file servers and application servers located at the Massachusetts Information Technology Center (MITC) in Chelsea.

Our examination of controls at the MBAO focused on selected general controls, such as physical security, environmental protection, system access security, inventory control over IT resources, and business continuity planning, including on-site and off-site storage of backup copies of magnetic media.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12 of the Massachusetts General Laws, we performed an audit of selected information technology (IT) related controls at the Metro Boston Area Office for the period July 1, 2004 through April 29, 2008. The audit was conducted from November 28, 2007 through April 29, 2008. The scope of our audit included an examination of physical security and environmental protection at the administrative office in Boston, system access security for MBAO's automated systems, inventory control for computer equipment and software, and business continuity planning, including provisions for the on-site and off-site storage of backup copies of magnetic media. In conjunction with our audit, we reviewed IT-related policies and procedures for areas under review.

Audit Objectives

Our primary audit objective was to determine whether adequate controls were in place to provide reasonable assurance that IT resources would be safeguarded, properly accounted for, and available when required. We sought to determine whether appropriate security controls were in place and in effect to provide reasonable assurance that only authorized parties could access IT resources and automated systems. We sought to determine whether adequate physical security controls were in place and in effect to restrict access to IT resources to only authorized users in order to prevent unauthorized use, damage, or loss of IT assets. We determined whether sufficient environmental protection controls were in place to provide a proper IT environment to prevent and detect damage or loss of IT resources. In addition, we determined whether adequate controls were in place to provide reasonable assurance that only authorized users were granted access to network resources, including the Mental Health Information System and other business-related office applications, and that procedures were in place to prevent and detect unauthorized access to automated systems. Another objective was to review and evaluate control practices regarding the accounting for computer equipment and software.

We sought to determine whether adequate business continuity planning had been performed and whether disaster recovery and business continuity plans were in place to restore mission-critical and essential business operations in a timely manner should the automated systems be unavailable for an extended period. In conjunction with our examination of business continuity planning, we determined whether adequate control procedures were in place regarding on-site and off-site storage of backup copies of magnetic media processed on file servers at the MBAO.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of MBAO's mission and business objectives. To gain an understanding of the primary business functions that were supported by the automated systems, we conducted pre-audit interviews with the managers and staff and reviewed MBAO's enabling legislation, Department of Mental Health's website, and selected documents, such as the "DMH Security Handbook," as of September 2007. Through interviews we gained an understanding of the information technology used to support MBAO's business operations. We documented the significant functions and activities supported by the automated systems and reviewed automated functions related to operations designated as mission-critical or essential.

We interviewed MBAO management to discuss internal controls regarding physical security and environmental protection over and within the administrative office and file server room housing computer equipment and the on-site and off-site storage areas for backup copies of magnetic media in Boston. We inspected the administrative office and the file server room in Boston, reviewed relevant documents, and performed selected preliminary audit tests. In conjunction with our review of internal controls, we performed a high-level risk analysis of risks and threats to selected components of the IT environment. We developed our audit scope and objectives based on our pre-audit work that included an understanding of MBAO's mission, business objectives and use of IT technology.

As part of our audit work, we reviewed the organization and management of DMH's IT operations that support MBAO's business functions. In that regard, we reviewed relevant policies and procedures, reporting lines, and IT-related job descriptions. In conjunction with our audit, we determined whether written, authorized, and approved policies and procedures for control areas under review had been implemented. We determined whether the policies and procedures provided management and users sufficient standards and guidelines to describe, review, and comply with statutes, regulations, generally accepted control objectives for IT operations and security, and policy directives, such as "DMH Security Handbook." Regarding our review of IT-related procedures, we interviewed senior management and staff, and completed internal control questionnaires. We obtained and reviewed an IT strategic plan prepared by DMH's Applied Information Technology Division that addressed IT services for MBAO.

To determine whether adequate controls were in effect to prevent and detect unauthorized access to the business offices housing automated systems, we inspected physical access controls, such as locked entrance and exit doors, the presence of security officers at the entrance to the building housing the MBAO office, and whether visitors were required to sign in and out. We reviewed access control procedures, such as the list of staff authorized to access the administrative office and file server room in

Boston and the presence of cameras and intrusion alarms. In addition, we reviewed control procedures regarding the keypad combination lock affixed to the door of the file server room and key management of physical keys distributed to MBAO managers and staff.

To determine whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (e.g., sprinklers and inert-gas fire suppression systems), an uninterruptible power supply, surge protectors for automated systems, and emergency power generators and lighting installed in the administrative office and file server room. We reviewed general housekeeping procedures to determine whether only appropriate office supplies and equipment were placed in the file server room or in the vicinity of computer-related equipment. To evaluate temperature and humidity controls, we determined whether appropriate dedicated air conditioning units were present in the file server room. Furthermore, we checked for the presence of water detection devices within the file server room, and whether the servers and other computer equipment were on racks raised above floor levels to prevent water damage.

With respect to system access security, our audit included a review of access privileges of those employees authorized to access the network and associated application systems. To determine whether MBAO's control practices regarding system access security adequately prevented unauthorized access to automated systems, we initially sought to obtain policies and procedures regarding system access and data security. We reviewed security practices with the with the Interim IT Coordinator, who was responsible for controlling access to MBAO's network resources and evaluated selected access controls to the network and applications available through the network. In addition, we reviewed DMH's control procedures regarding remote access privileges to the network for MBAO personnel. We determined whether MBAO's internal control documentation included control practices, such as an acceptable use policy for IT resources and security awareness training. We interviewed MBAO managers and staff and DMH personnel regarding the control and monitoring of the MBAO's network, including security procedures regarding system access to the automated systems.

To determine whether the administration of logon ID and passwords was being properly carried out, we reviewed and evaluated control practices regarding system access security. We reviewed the security procedures with IT personnel for access to the MHIS and other business-related applications. We reviewed control practices used to assign MBAO staff access to network resources, including the MHIS and the Massachusetts Management Accounting and Reporting System (MMARS). To determine whether adequate controls were in place to ensure that access privileges to the automated systems were

granted to only authorized users, we reviewed and evaluated procedures for authorizing and activating access to application software and related data files.

To determine whether selected users with active privileges were current employees or outsourced staff, we obtained the list of individuals granted access privileges to the MHIS and MMARS and compared 21 (100%) users (e.g., nine employees and 12 outsourced staff) granted access to MHIS to the personnel roster of current employees or the list of contractors provided by the Public Consulting Group. Further, 15 employees who had been granted access to MMARS, as of December 22, 2007 were compared to the current roster of current employees. We determined whether all employees authorized to access the automated systems were required to change their passwords periodically and, if so required, we reviewed the frequency of the changes. We determined whether appropriate user ID and password administrative procedures were followed, such as appropriate password composition and length.

Regarding inventory control over IT resources, we first reviewed formal policies and procedures promulgated by the Massachusetts Office of the State Comptroller (OSC) regarding inventory control. To determine whether IT-related resources were being properly safeguarded and accounted for, we reviewed the roles of the DMH's Applied Information Technology and MBAO personnel regarding the accounting for computer equipment and software, reviewed the inventory control procedures for these IT resources, and performed selected tests. During our fieldwork, we obtained the hardware inventory record, as of December 31, 2007, from the Interim IT Coordinator. At that time, servers, workstations, and notebook computers listed on the record were valued at $227,964. We determined whether computer equipment installed at the administrative office in Boston was tagged with state identification numbers and whether the Office's inventory record accurately reflected tag numbers and equipment serial numbers. We reviewed the inventory record to determine whether appropriate "data fields," such as state identification number, manufacturer's model number, serial number, location, and cost were included for each piece of equipment listed in the record and provided sufficient information to identify and monitor computer equipment. We also performed data analysis on the inventory record to identify any duplicate records, unusual data elements, or missing values.

To determine whether the hardware inventory record, as of December 31, 2007, accurately reflected computer equipment installed in Boston, we initially reviewed the 382 pieces of computer equipment listed on the record. We selected a statistical sample of 60 (15.8%) of 382 workstations listed on the record that were located in Boston for review. We compared the tag numbers and serial numbers attached to the computer equipment to the corresponding numbers listed on the hardware inventory record. We determined whether serial numbers were accurately recorded on the record. Moreover, to

assess the integrity of MBAO's inventory record, we selected a judgmental sample of 16 pieces of computer equipment installed at the Boston office and determined whether the IT equipment had been properly assigned asset numbers, were tagged, and were properly recorded on the inventory record. We confirmed the 11 (100%) servers listed on the hardware inventory record to the actual equipment installed at the MBAO. We also determined whether any computer equipment had been designated as surplus or disposed of during our audit period.

With respect to notebook computers, we initially determined the role of the MBAO regarding the management and control of the computers. We reviewed control procedures for assigning the six notebook computers to MBAO managers. To gain an understanding of control procedures regarding the distribution to and return of the notebook computers from Office staff, we interviewed the Area Operations Manager.

To determine whether MBAO complied with the Office of the Massachusetts State Comptroller's regulations regarding accounting for fixed assets, we reviewed evidence supporting MBAO's performance of an annual physical inventory. In addition, we sought to determine whether MBAO's staff were aware of, and in compliance with, Chapter 647 of the Acts of 1989 reporting requirements for missing or stolen asset. We reviewed documented inventory control policies and procedures, interviewed senior management to determine whether MBAO had had any incidences of missing or stolen IT-related equipment during the audit period, and verified whether any incidents were reported to the Office of the State Auditor.

To assess disaster recovery and business continuity planning, we reviewed the adequacy of formal business continuity plans to restore mission-critical and essential operations in a timely manner should the automated systems be unavailable for an extended period. We interviewed the Interim IT Coordinator and the Area Operations Manager 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 and evaluated the DMH Dr. Solomon Carter Fuller Mental Health Center "Emergency Preparedness Plan, as of October 2007 and the DMH "AIT Emergency Response and Support Plan," as of December 2007. According to the Area Operations Manager and the Interim IT Coordinator, the DMH "Emergency Preparedness Plan," designed by the Dr. Solomon Carter Fuller Mental Health Center, was serving as the Continuity of Operations Plan (COOP). According to the "Emergency Preparedness Plan," the document had been prepared consistent with standards and guidelines promulgated by the Massachusetts Emergency Management Agency (MEMA) and the Federal Emergency Management Emergency Agency (FEMA).

According to MEMA, "the COOP should be prepared in accordance with Department of Homeland Security Headquarters COOP Guidance Document, as of April 2004, that provides a structure for formulating a COOP plan; Presidential Decision-67, "Ensuring Constitutional Government and Continuity of Operations," which requires all Federal Departments and agencies to have a viable COOP capability; and Commonwealth of Massachusetts Executive Order No. 144 that requires all Commonwealth agencies and local communities to prepare for emergencies and disasters, and to provide emergency liaisons to MEMA for coordinating resources, training, and operations." We determined whether the "Emergency Preparedness Plan" and other business continuity documents included sufficient information to support the resumption of the MBAO's normal business operations in a timely manner.

To determine whether controls were adequate to ensure that software and data files for business applications would be available should the automated systems be rendered inoperable, we interviewed the Interim IT Coordinator and staff responsible for generating backup copies of magnetic media. Furthermore, we reviewed the adequacy of provisions for on-site storage of backup copies of mission-critical and essential magnetic media at the administrative office in Boston. We reviewed procedures for transferring to and retrieving backup copies from the off-site storage location. We inspected the MBAO's file server room and reviewed the adequacy of physical security and environmental protection controls over the backup media stored in the room. We did not review the off-site storage location for backup copies generated at MBAO. Furthermore, we did not review ITD backup procedures for transactions processed through the Massachusetts Management Accounting and Reporting system (MMARS) and the Human Resources Compensation Management System (HR/CMS) or the MHIS processed at the Massachusetts Information Technology Center (MITC). To determine whether backup copies of magnetic media stored on-site were adequately safeguarded from damage or loss, we reviewed physical security over the on-site storage location through observation and interviews with MBAO managers and DMH IT personnel.

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

AUDIT CONCLUSION

Based on our audit at the Metro Boston Area Office, we found that IT resources, including the file servers and workstations installed at the administrative office in Boston, were adequately safeguarded, environmentally protected, and properly accounted for. We determined that appropriate control practices regarding logon ID and password administration were in place to help provide reasonable assurance that only authorized parties could access network resources. Although we found that the Department of Mental Health had documented important controls regarding business continuity planning, such as the designation of alternate processing sites, MBAO needed to strengthen controls, in conjunction with DMH, to provide reasonable assurance that normal business operations could be resumed in a timely manner should automated resources be unavailable for an extended period. Moreover, we determined that on-site storage needed to be improved for backup copies of magnetic media at the administrative office in Boston.

Our audit found that adequate physical security controls were in place over and within the administrative office in Boston and the file server room to provide reasonable assurance that access to IT resources would be restricted to only authorized persons and that IT resources would be safeguarded from damage or loss. We determined that security officers were on duty 24/7 for the building housing the Dr. Solomon Carter Fuller Mental Health Center, visitors were required to sign in prior to entering the building's business offices, and that cameras and intrusion detection devices were installed in appropriate locations. We found that appropriate key management controls were in place for MBAO business offices. We determined that the file server room was locked by means of a punch keypad lock and a separate physical key, the room was kept locked, and that access was restricted to selected DMH and MBAO staff.

We determined that adequate environmental protection controls, such as smoke detectors and fire alarms, were in place in the Dr. Solomon Carter Fuller Mental Health Center to help prevent damage to, or loss of, IT resources. Emergency procedures were posted in the administrative office and, according to MBAO management, staff had been trained regarding emergency shutdown procedures during the prior two years. Our audit disclosed that the file server room was well organized, temperature and humidity levels within the room were appropriate, and an uninterruptible power supply (UPS) device was in place to permit a controlled shutdown and to prevent a sudden loss of data. The servers were placed on a rack above floor level to prevent water damage and a fire suppression system was installed in the room. A

hand-held fire extinguisher was located within the server room. We agree with management's decision to upgrade water detection controls in the file server room.

Regarding systems access security, we found that appropriate control practices regarding the authorization of personnel to be granted access to network resources, activation of access privileges through the granting of a logon ID and password, and deactivation of access privileges were in place. We found controls in place so that access privileges would be deactivated or appropriately modified should MBAO employees terminate employment or incur a change in job requirements. A security officer was designated; policies and procedures were documented; and MBAO staff were required to participate in formal security training, sign a formal security statement regarding password protection and confidentiality, and pass a security-related test. Our tests confirmed that users granted access to MHIS were MBAO employees or outsourced staff and that only current MBAO employees had access to MMARS. We determined that adequate policies and procedures were in place for password formation, use and frequency of change.

With respect to inventory control over computer equipment, we found that MBAO's control practices provided reasonable assurance that IT resources were properly accounted for in the inventory system of record. We determined that the inventory system of record for computer equipment, as of December 31, 2007, could be relied upon as a current, accurate, complete, and valid record of computer equipment installed at MBAO. We determined that a list of software licenses was maintained. Our review of compliance with Chapter 647 of the Acts of 1989 reporting requirements for missing or stolen Commonwealth assets revealed that MBAO staff responsible for inventory were aware of the requirements and that MBAO did not have any reported occurrences of missing or stolen computer equipment during the audit period. Regarding six notebook computers assigned to senior managers, we recommend that to improve controls MBAO maintain sign-in/out logs for all notebook computers and that the status of the computers be periodically monitored.

Regarding business continuity planning, we found that the MBAO was not adequately covered by an approved, comprehensive, and tested business continuity plan to address the loss of IT systems and processing capabilities. Our audit revealed that DMH had documented important control practices in the "Dr. Solomon Carter Fuller Mental Health Center Emergency Preparedness Plan" and the DMH "Applied IT Emergency Response and Support Plan." The "Emergency Preparedness Plan" documented detailed emergency/evacuation plans and the "Applied IT Emergency Response and Support Plan." listed mission-critical systems, information related to restoration of IT services, instructions regarding a declaration of an emergency, and a contact list. In addition, DMH had designated two alternate processing sites.

To strengthen business continuity controls, we recommend that MBAO, in conjunction with DMH Headquarters, address the following control weaknesses: perform a criticality assessment and risk analysis; develop a list of all potential disaster scenarios and instructions to follow for each event, document a list of vendors, and enhance the emergency contact list to include appropriate MBAO personnel. MBAO should develop user area plans, specific documented plans and procedures for each business unit, to use when automated systems are not available. In addition, MBAO should provide a secure and environmentally protected location for on-site storage.

AUDIT RESULTS

Business Continuity Planning

Our audit disclosed that although DMH had documented certain important control practices regarding business continuity planning in the "Dr. Solomon Carter Fuller Mental Health Center Emergency Preparedness Plan," as of October 2007 and the DMH "Applied IT Emergency Response and Support Plan, "as of December 2007, none of the written documentation provided sufficient recovery strategies or resources to restore normal business operations in a timely manner should automated systems be unavailable for an extended period. We found that, although backup procedures for magnetic media processed on the file servers at the administrative office were adequate, controls regarding on-site storage of magnetic media needed to be improved. Depending on the nature and extent of a loss of IT systems or processing, the Area Office could experience difficulties in regaining mission-critical and essential business processes within an acceptable period of time given the absence of a sufficiently comprehensive recovery and business continuity plan specific to MBAO.

Weaknesses pertaining to business continuity-related control practices included, but were not limited to DMH's and MBAO's need to:

- Perform a criticality assessment and risk analysis;
- Document all potential disaster scenarios and instructions to follow for each specific event;
- Develop detailed procedures for establishing and relocating personnel to an alternate site, including designated staff for each site, supplies and equipment;
- Develop a contact list, including IT personnel to be notified in the event of an emergency with all communication information, such as landline telephone numbers, cell phone, and e-mail;
- Develop user area plans documenting procedures to follow for each business unit should automated systems be unavailable so that business activities can continue;
- Document detailed procedures regarding restoration of network services; and
- Develop schedules for testing a comprehensive business continuity plan, and document the tests performed and any corrective action taken.

We determined that, at the close of our audit, DMH had developed detailed emergency/evacuation plans for the Dr. Solomon Carter Fuller Mental Health Center in which the MBAO administrative office is located, listed mission-critical systems and had designated two alternate processing sites.

To a degree the "Dr. Solomon Carter Fuller Mental Health Center Emergency Preparedness Plan" and the "Applied Emergency Response and Support Plan" addressed important elements fundamental to business continuity planning, such as emergency/evacuation procedures, a listing of essential business functions,

designation of the MBAO's mission-critical systems, notification procedures, contact information, and some detail on responsibilities for continuity of operations.

We found that MBAO had implemented on-site storage of backup copies of magnetic media for data files residing on MBAO workstations, and that DMH had established procedures for on-site and off-site storage of backup copies of magnetic media for systems under their charge. Although MBAO had on-site storage of backup media, environmental controls over the backup media needed to be improved.

The objective of business continuity planning is to help ensure the continuation of mission-critical and essential functions enabled by technology should a disaster cause significant disruption or loss of computer or network operations. Generally accepted industry practices and standards for computer operations support the need to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans as required.

Contingency planning should be viewed as a process to be incorporated within the functions of the organization rather than as a project completed upon the drafting of a written plan. Since the criticality of systems may change, a process should be in place that will identify a change in criticality or other factors, such as risk, and amend the business continuity and contingency plans accordingly. In addition, changes to the overall IT infrastructure and user requirements should be assessed in terms of their impact to existing disaster recovery and business continuity plans.

An effective disaster recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios. Appropriate user area plans should outline recovery or contingency steps with detailed steps to be followed to efficiently restore business operations. The area plans should be coordinated with overall enterprise-based disaster recovery and business continuity plans.

Recommendation:

We recommend that to strengthen business continuity planning, MBAO, in conjunction with DMH Central Office, should:

- Gain a better understanding of generally accepted computer industry standards, such as Control Objectives for Information Technology (CobiT) regarding disaster recovery and business continuity-planning, and recovery and contingency objectives and procedures for mission-critical and essential business operations. Generally accepted control practices would include a criticality assessment and risk analysis, policies; procedures; assurance mechanisms; defined responsibilities; and organizational controls, such as steering committee, recovery teams, and oversight functions. The framework should also include senior management assignment of enterprise responsibility for additional recovery strategies and adequate provisions for on-site and off-site storage.
- Perform an enterprise-based risk analysis and criticality assessment to ensure that all functional areas and business processes supported by technology are evaluated and update, if necessary, the risk analysis results for IT operations. The risk analysis and criticality assessment should include all external partners, such as the federal government and outsourced services, such as those provided by the Executive Office for Administration and Finance's Information Technology Division (ITD).
- Review the list of disaster scenarios regarding the loss of IT systems that would impact MBAO operations and business functions. Develop and update recovery and business continuity strategies for each of the disaster scenarios identified.
- Reconfirm MBAO's 's understanding of the relative importance of business functions and the potential impact of a loss IT processing support. MBAO should formally rank mission-critical, essential, and less essential business process functions and IT processes for development and update of disaster recovery, business continuity, and contingency plans.
- Obtain an understanding and adequate level of assurance of disaster recovery and business continuity plans for required services and support from all mission-critical and essential business partners and third-party providers.
- Establish a single organizational framework to which business process area plans and IT plans can be linked to an overall business continuity plan. In conjunction with the development of the business continuity plan, MBAO should establish targets for acceptable time periods by which mission-critical IT operations and business functions need to be recovered.
- Ensure that appropriate resources are available at alternate processing sites, such as suitable hardware and communication equipment; supplies; adequate space in which to resume operations; timely accessibility of backup copies of all required application programs, data files and system utilities; documented policies and procedures; and sufficient personnel.
- Develop and perform appropriate levels of testing to provide MBAO with sufficient assurance as to the viability of recovery and business continuity plans. Tests should be performed on control practices that can be reviewed and evaluated independently of the test of recovery strategies in conjunction with the implementation of the alternate processing site. Once tests are completed, test results should be reviewed against expected test plan results and reviewed and approved by business process operations and IT management.

- Review business continuity requirements periodically or upon major changes to user requirements regarding the automated systems. We recommend that subsequent to testing the business continuity plan, the plan should be updated when needed to provide reasonable assurance that it is current, accurate, and complete. The completed plan should be distributed to all appropriate staff members, including DMH and MBAO officials, senior management, IT staff, and ITD administrators and staff.
- Train the MBAO staff in the execution of the business continuity plan under emergency conditions. Ensure that all key business process and IT management and staff have adequate skill and knowledge to carry out all tasks and activities outlined in recovery and business continuity plans.
- Strengthen controls over on-site copies of magnetic media stored at the administrative office.

Auditee's Response:

The Department of Mental Health has participated in a number of site and area office audits over the past several months and benefited from the lessons learned by those experiences. One of these is the audit relative to DMH Metro Boston Area Office located in the Dr. Solomon Carter Fuller Mental Health Center. DMH has reviewed in detail the draft document, No. 2008-0242-4T, Office of the State Auditor's Report on the Examination of Information Technology Related Controls at the Department of Mental Health Metro Boston Area. We offer the following DMH responses to the findings offered by the State Auditor's team:

IT Backup Environment and Practices:
DMH has refreshed a substantial share of its environment over the past two years. One element is the backup support. The process was reviewed by the Auditors and was found to be strong and based on sound industry standards with the exception of our off-site storage practices. DMH does rotate its media off site on a weekly basis, but our previous site practices often moved tapes within the same building, or campus on which the tapes were produced. This was found to be insufficient and DMH agrees. DMH now moves all media for all locations on a weekly rotation to a locked location within DMH AIT control at the Hadley building in Westborough. Media produced at the Hadley location are stored in a locked area at the Westborough State Hospital (building separated by public roads and a number of private properties). The final elements of the plan to be completed:

- *An assessment of the locked storage container for fire retardant and heat retardant status*
- *The storage containers to be used during transport of the media between sites*

DMH will finalize these two remaining elements within the financial capabilities of DMH within this fiscal year.

Business Continuity Planning:
Like all Commonwealth agencies, DMH needs to improve its focus on the Business Continuity needs and planning required to support its users and clients under all circumstances as defined in Executive Order No. 490 for Continuity of Operations and Business Continuity Planning. DMH AIT has negotiated and agreed to a project scope

for AIT's participation in DMH Business Continuity Planning. DMH AIT will assume responsibility for completing a comprehensive Information Technology Service Continuity Management (ITSCM) Plan. This approach, as defined by the IT industry, is an approach, which insures an organization's ability to continue to provide a pre-determined and agreed level of IT Services to support the minimum business requirements, "Service Continuity". The intent is to then use and include the ITSCM in all site Business Continuity Plans and the greater DMH-wide Business Continuity Plans. The following is the basic plan and timeline for the ITSCM, which is currently in progress:

Overall Process Strategy:

Define direction and high-level methods to meet IT service level objectives

- *Establish generic framework and guidelines for a continuity program, including:*
  - *Management structure & responsibilities (in progress)*
  - *How to conduct business criticality & risk assessments (in progress)*
  - *How to define and create an IT Service Continuity plan*
  - *How to rehearse an IT Service Continuity plan*
  - *Solution architectures and design considerations*
  - *Document and include in all site response plans to any area of business continuity or disaster recovery*

Agreed at Executive – CO and Area levels

Needs to consider four stages of major incident

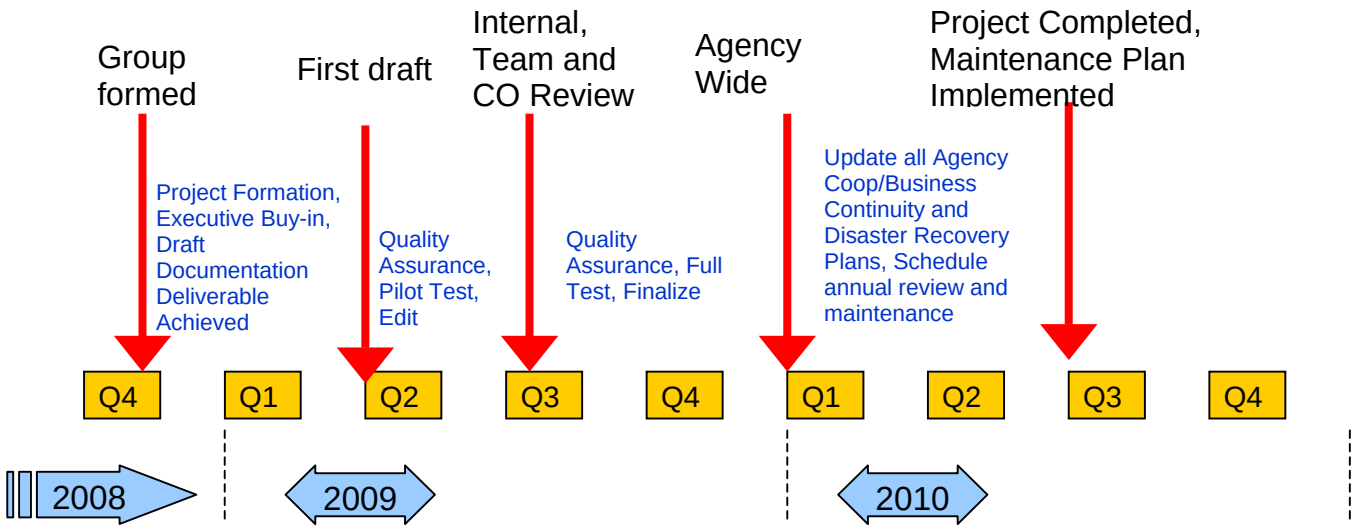
- *Initial response*
- *Service recovery*
- *Service delivery (following incident)*
- *Normal service resumption*

Manage and Launch the Process

- *Identify and document for all of DMH*
- *Standardize on a state-wide approach*
- *Build IT disaster recovery and business continuity planning into the design process*
- *Build incident specific work flows using a standard approach and template*
- *Standardize all response tasks and documentation requirements*
  - *Detail all services and applications and determine the importance to DMH and a clearly defined order of restoral*
  - *Establish Recovery Objectives (point in them and outage tolerance) for all services and applications*
- *Educate and train – executives, participants and all others at appropriate levels*
  - *Expectations*
  - *Process*
  - *Deliverables*
- *Equip everyone involved appropriately to meet their responsibilities*
- *Build a comprehensive test plan that is exercised to some level quarterly*
- *Test – correct – test again*
- *Deploy the plan for inclusion in ALL Emergency Preparedness/Disaster Recovery/Business Continuity/Area/Site/DMH-wide/Department plans*
- *Participate in non-DMH tests using our tests to gain peer input (example: EOHHS, DPH, ITD testing opportunities*

- *Review and maintain the documentation on a yearly basis (at a minimum)*

Timeline for ITSCM:



The Department of Mental Health would like to express our appreciation to the Auditors for this opportunity to clarify our approach to meeting our obligations in support of the Commonwealth's constituents and look forward to the final report.

Auditor's Reply:

We are pleased that DMH has strengthened controls over its off-site storage location for backup copies of magnetic media. Furthermore, we concur with DMH management's decision to improve temperature and humidity controls regarding storage containers used to transport backup tapes and store them at the off-site location. We continue to recommend that MBAO maintain a secure and environmentally protected on-site location for backup copies of magnetic media to ensure constant availability of data files and software.

We concur with DMH's management decision to develop a comprehensive Information Technology Service Continuity Management (ITSCM) Plan to provide predetermined IT services to support "Service Continuity" and to include the ITSCM Plan in all future business continuity planning. We are pleased that DMH's framework includes important procedures, such as performing a risk analysis and criticality assessment, training appropriate staff, and testing the plan periodically.

We will review the status of business continuity at our next IT audit.

Department of Mental Health
Metro Boston Area Office
Summary of Internal Control Practices
as of April 29, 2008

Pg Ref	Control Area	Control Objective	Control Activities	Status of Control	Documented Controls	Adequacy of Documentation
9	Physical Security	Provide reasonable assurance that only authorized staff can access business offices and file server room, to prevent unauthorized use, loss or damage to IT resources or sensitive documentation,	Control over access to business offices, file server room, file servers and computer equipment; designated facilities manager; intrusion detection devices; locked doors, security officers on duty,	In Effect	Yes	Adequate
9	Environmental Protection	Provide reasonable assurance that IT-related resources operate in an appropriate environment and are adequately protected from loss or damage	Proper ventilation, temperature and humidity controls, fire alarms, smoke detectors, fire suppression mechanisms, water detection devices, water sprinklers, UPS, posted emergency procedures	In Effect	Yes, for Emergency and Evacuation Procedures	Inadequate, additional documentation needs improvement
10	System Access Security	Provide reasonable assurance that only authorized users are granted access to the automated systems and that logon IDs and passwords are deactivated for users no longer needing access	Passwords required to access automated systems, changes of passwords required at least every 60 days; formal rules for password formation and use; documented procedures for deactivation of logon IDs and passwords, users required to sign “use of IT Resources”	In Effect	Yes	Adequate
10	Inventory Control over IT-related Resources	Provide reasonable assurance that IT-related resources are properly safeguarded, accounted for in the inventory record.	Maintenance of an up-to-date inventory record; hardware tagged with state ID tags; control procedures documented for notebook computers; annual physical inventory and reconciliation performed	In Effect	Yes	Adequate

Department of Mental Health
Metro Boston Area Office
Summary of Internal Control Practices
as of April 29, 2008

Pg Ref	Control Area	Control Objective	Control Activities	Status of Control	Documented Controls	Adequacy of Documentation
10, 12	Business Continuity Planning	Provide reasonable assurance that mission-critical and essential functions can be restored in a timely manner should file servers and microcomputer workstations be rendered inoperable or be inaccessible.	Current, formal, tested business continuity plan; alternate processing site; periodic review and modification of plan; plan implemented and distributed to appropriate staff; and staff trained in its use	Insufficient	Yes	Inadequate
10, 12	On-site storage for backup copies generated at MBAO	Provide reasonable assurance that backup copies of magnetic media are available should computer systems be rendered inoperable or inaccessible	Magnetic media backed up nightly; schedule for creating backups, appropriate records maintained of backup; physical access security and environmental protection of storage are adequate; storage area is a separate on-site location	Adequate, except for certain environmental controls over storage area	Yes	Inadequate
13	Off-site storage for backup copies generated at MBAO	Provide reasonable assurance that critical and important backup copies of magnetic media are available should computer systems be rendered inoperable or inaccessible	Schedule for creating backups, storage area in a separate off-premises location, schedule for distribution to off-site location and return of backup tapes.	Adequate	Yes	Inadequate

Status of Control-Key:

In Effect = Control in place sufficient to meet control objective.

None = No internal control in place.
Insufficient = Partial control in place but inadequate to meet control objective.

Adequate = Standard or guideline sufficient to describe, review, and follow significant controls.
Inadequate = Standard or guideline insufficient to describe, review, and follow significant controls.
N/A = Not Applicable