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. 2008-0253-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE DEPARTMENT OF MENTAL HEALTH'S ERICH LINDEMANN MENTAL HEALTH CENTER

July 1, 2006 through February 28, 2009

OFFICIAL AUDIT REPORT
JULY 28, 2009

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. The DMH and its organizational units are placed under the purview of the Executive Office of Health and Human Services.

The Metro Boston Area (MBA), which is comprised of the Metro Boston Area Office (MBAO), three mental health centers, including the Erich Lindemann Mental Health Center, and four local service sites in Boston and Cambridge, as well as inpatient units at the Lemuel Shattuck Hospital, serves the cities of Boston, Cambridge, Chelsea, Revere, Somerville, and the towns of Brookline and Winthrop. The primary mission of the MBA's mental health centers is to provide comprehensive inpatient and/or outpatient mental health services and support services to meet the needs of clients requiring care for mental illness. Metro Boston Area mental health centers also provide emergency evaluation and assessment, short-term and long-term inpatient and/or outpatient care, and forensic evaluations required by Massachusetts courts and rehabilitative and support services in a community setting.

Through vendor contracts and state-operated programs, the Erich Lindemann Mental Health Center (hereinafter referred to as the ELMHC or the Lindemann) provides a variety of client services, such as community outreach, outpatient counseling, and residential and transitional housing programs. For example, the Parker Shelter West, located at the Lindemann, opened in January 2009 and provides 20 beds for women. The Homeless Outreach Team's case managers provide homeless persons with temporary housing and counseling at ELMHC, the Freedom Trail Clinic provides outpatient counseling, the West End Shelter provides temporary housing, and the Metro Boston Legal Office offers legal assistance. As of December 16, 2008, all inpatients located at the Erich Lindemann Mental Health Center were transferred to the Dr. Solomon Carter Fuller Mental Health Center in Boston. The ELMHC, certified as a hospital, is staffed by a Site Director, a Director of Risk Management and Quality Assurance, two supervisors, and 69 employees. DMH police and business office staff who are located at the Lindemann report to the MBAO.

Of the $130,925,814 expended for the MBA for the 2008 fiscal year, $26,327,824 was expended by ELMHC. According to DMH, $27,312,012 was received for the same period from client services/third-

party billings for MBA. ELMHC received $1,871,482 of this amount. Regarding information technology (IT), MBA expended $1,190,227, including purchases for Lindemann.

At the time of our audit, ELMHC's computer operations were supported by 27 file servers and 158 workstations installed throughout the administrative office that were configured in a local area network (LAN). Of the 27 file servers, six were dedicated to Lindemann operations, 13 were dedicated to the DMH Central Office functions, and eight were dedicated to both ELMHC and DMH Central Office processing activities. The file servers were connected to a wide area network (WAN) that provided access to the Massachusetts Management Accounting and Reporting System (MMARS), Human Resources Compensation Management System (HR/CMS), and additional network services, including e-mail, that are supported by the Commonwealth's Information Technology Division. In addition to the workstations available for ELMHC personnel, there were three notebook computers assigned to senior managers. Overall IT operations and services supporting the ELMHC were provided by DMH's Applied Information Technology (AIT) Division.

The primary application used by ELMHC 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 inpatient 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. According to DMH management, other critical applications include e-mail and MMARS.

The Office of the State Auditor's examination of controls at the ELMHC 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 Erich Lindemann Mental Health Center for the period July 1, 2006 through February 28, 2009. The audit was conducted from May 19, 2008 through February 28, 2009. The scope of our audit included an examination of physical security and environmental protection at the administrative office, system access security for ELMHC's automated systems, inventory control over 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 the 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 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. 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 to prevent unauthorized use, damage, or loss of IT resources. In addition, 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. Another objective was to review and evaluate inventory control practices regarding the accounting for computer equipment and to determine whether there was a list maintained of 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 residing on ELMHC's file servers.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of ELMHC'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 DMH's enabling legislation, the Department of Mental Health's website, ELMHC's mission and business functions, 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 ELMHC'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 ELMHC management to discuss internal controls regarding physical security and environmental protection over and within the administrative office, the file server room housing computer equipment, and the on-site and off-site storage areas for backup copies of magnetic media. We inspected the administrative office and the file server room, 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 selected components of the IT environment.

We reviewed selected functions of DMH's Applied Information Technology (AIT) operations that supported ELMHC's business operations. In that regard, we reviewed relevant policies and procedures, reporting lines, and IT-related job descriptions. We developed our audit scope and objectives based on our pre-audit work that included an understanding of ELMHC's mission, business objectives, and use of IT.

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. Regarding our review of IT-related procedures, we interviewed selected DMH and ELMHC management and staff and completed questionnaires regarding selected IT internal controls.

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 DMH police officers at the entrance to the building housing the

ELMHC administrative 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 file server room, and inspected for the presence of cameras and intrusion alarms. In addition, we reviewed control procedures regarding access to the file server room, including management of physical keys distributed to DMH Central Office staff authorized to access the room, and controls over the keypad combination lock for the door of the file server room.

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, 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 and whether temperature and humidity were regulated and continuously monitored. Furthermore, we checked for the presence of water detection devices within the file server room, and whether the servers and other computer equipment were placed 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 ELMHC'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 Acting IT Operations Manager and LAN Administrator, who were responsible for controlling access to ELMHC's network resources. Furthermore, we evaluated selected access controls to the network and application systems residing on the network. In addition, we reviewed access privileges for ELHMC or outsourced staff who had been granted remote access to network resources. We determined whether ELMHC's internal control documentation included control practices, such as an acceptable use policy for IT resources and security awareness training. We interviewed DMH Central Office personnel regarding the control and monitoring of the network, including security procedures regarding system access to the automated systems.

To determine whether the administration of logon ID and passwords were 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 ELMHC staff access to network resources, including the MHIS. We determined whether ELMHC staff had been granted access to the Massachusetts Management Accounting and Reporting System (MMARS).

To determine whether adequate controls were in place to provide reasonable assurance 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. We sought to determine whether appropriate procedures were in place to document the authorization of staff to be granted access privileges to network resources. At the inception of our audit, we selected a statistical sample of 25 (9.84%) of 254 users and reviewed documentation for authorization to be granted access privileges to the network. During our audit, all inpatients and a significant number of staff at the Lindemann were transferred to the Dr. Solomon Carter Fuller Mental Health Center. Audit tests regarding deactivation of access privileges were performed after the transfer of inpatients and staff. To determine whether selected users with active privileges were current employees, we obtained the list of individuals granted access privileges to the MHIS and compared all 69 (100%) ELMHC users granted access to MHIS to the personnel roster of current employees, as of February 28, 2009. We determined whether any outsourced staff, as of February 28, 2009, were granted access privileges to network resources. Another objective was to determine whether all employees authorized to access the automated systems were required to change their passwords periodically and the frequency of the changes. We sought to determine whether appropriate procedures regarding password formation and use, such as proper password composition and length, were followed.

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 AIT and ELMHC personnel regarding the accounting for computer equipment and software, reviewed the inventory control procedures for IT resources, and performed selected tests. We reviewed DMH procedures for the leasing and receipt of computer equipment, the transfer of the equipment to area offices and local service sites, testing, tagging of items with state identification numbers, and the installation of workstations.

As part of our audit fieldwork, we reviewed the DMH procedures for the agency-wide leasing of 6,403 pieces of computer-related equipment, identified as central processing units (CPU), monitors, workstations, and notebooks, with a listed value, as of July 2006, of $2,531,317. We found that of the

6,403 IT-related items, 3,440 items consisted of CPUs and monitors. We determined that of the 3,440 items, 310 pieces of computer equipment, consisting of 158 CPUs and 152 monitors, were installed at ELMHC. Because the documentation for the agency-wide lease did not specifically indicate which pieces of computer equipment had been installed at ELMHC, we could not test a specific leased item to the Center's inventory record, as of June 6, 2008, and to the actual item on hand. Based upon the costs listed for CPUs and monitors on the DMH lease agreement, we estimated the listed value of the 158 CPUs and 152 monitors installed at ELMHC to be $112,154.

During our fieldwork, we obtained the hardware inventory record, as of June 6, 2008, from the Acting IT Operations Manager. As discussed above, the record included both leased CPUs and monitors and other prior purchases of computer-related equipment. 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 that sufficient information was provided to identify and monitor computer equipment. Furthermore, we determined whether computer equipment installed at ELMHC's administrative office was tagged with state identification numbers and whether the Lindemann's inventory record accurately reflected tag numbers and equipment serial numbers. 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 June 6, 2008, accurately reflected computer equipment installed in Boston, we initially reviewed the 359 pieces of computer equipment; specifically, CPUs, monitors, printers, and faxes listed on the record. We selected a statistical sample of 60 (16.7%) of the 359 pieces of equipment listed on the record 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 the serial numbers were accurately recorded on the record. Moreover, to further assess the integrity of ELMHC's inventory record, we selected a judgmental sample of 15 CPUs and five monitors located at the Boston office and determined whether the IT equipment had been properly assigned asset numbers, tagged, and was properly recorded on the inventory record. We confirmed that the three notebook computers and 27 (100%) servers listed on the hardware inventory record were in fact installed at the ELMHC. We determined whether any computer equipment had been designated as surplus or disposed of during our audit period.

With respect to notebook computers, we initially identified the role of managing and controlling computer equipment. We reviewed control procedures for assigning the three notebook computers to ELMHC managers. To gain an understanding of control procedures regarding the distribution to, and return of the

notebook computers from, Lindemann managers, we determined whether sign-out/in logs acknowledging staff responsibility for the assigned equipment and supervisory approvals were in place.

We sought to determine whether ELMHC was in compliance with the reporting of missing or stolen assets as required by Chapter 647 of the Acts of 1989. We reviewed documented inventory control policies and procedure and interviewed senior management to determine whether any IT equipment had been lost or stolen during the audit period. We determined whether missing equipment had been reported to the Office of the State Auditor, as required by Chapter 647 of the Acts of 1989.

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 Acting IT Operations Manger and DMH's Director of Information Technology Operations 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 initially reviewed the "Pandemic Influenza, Continuity of Operations Plan (COOP) for the Department of Mental Health" as of August 10, 2006. We reviewed and evaluated the DMH "AIT Emergency Response and Support Plan" as of December 2007, and the Erich Lindemann Mental Health Center's "Emergency Preparedness Plan" as of February 17, 2009. 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 Agency (FEMA). We also reviewed the "DMH Information Technology and Business Continuity Approach" as of December 2008, which provides a general framework for business continuity planning at DMH. We determined whether the "Emergency Preparedness Plan" and other business continuity documents included sufficient information to support the resumption of the ELMHC'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 Acting IT Operations Manger, DMH's Director of Applied Information Technology, and staff responsible for generating backup copies of magnetic media. 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. We inspected the ELMHC's file server room and reviewed physical security and environmental protection controls over the backup media stored in the room. We reviewed procedures for transferring to and retrieving backup copies from the off-site storage location. In conjunction with our evaluation of off-site storage for backup copies, we reviewed the

"DMH Enterprise Backup Plan" as of February 24, 2009, which documents the distribution to and return of backup copies of magnetic media from the off-site storage location. We did not review the off-site storage location for backup copies generated at ELMHC. Furthermore, we did not review the Executive Office for Administration and Finance's Information Technology Division (ITD) backup procedures for transactions processed through the Human Resources Compensation Management System (HR/CMS) or the MHIS processed at the Massachusetts Information Technology Center (MITC).

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 Erich Lindemann Mental Health Center (ELMHC), we determined that, with the exception of business continuity planning for automated systems, adequate controls were in place to appropriately safeguard and account for the Center's information technology (IT) resources. Our audit disclosed that IT resources, including the file servers and workstations installed at the administrative office, were adequately secured, environmentally protected, and properly accounted for in agency records. 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 and that control procedures regarding activation and deactivation of access privileges were appropriate.

Although we found that the Department of Mental Health (DMH) had developed important controls in a variety of business continuity-related documents, such as the "Pandemic Influenza, Continuity of Operations Plan (COOP) for the Department of Mental Health" as of August 10, 2006, and ELMHC "Emergency Preparedness Plan" as of February 17, 2009, the Lindemann needs to strengthen controls, in conjunction with DMH Central Office and the Metro Boston Area Office, to provide reasonable assurance that normal business operations could be resumed in a timely manner should automated resources be unavailable for an extended period. Our audit revealed that although on-site and off-site backup procedures for magnetic media residing on the workstations and file servers at the administrative office were adequate, environmental protection controls over on-site storage for backup copies need to be strengthened.

Our audit found that adequate physical security controls were in place over and within the administrative office and the file server room to provide reasonable assurance that access to IT resources would be restricted to only authorized persons and that IT assets would be safeguarded from damage or loss. We determined that DMH police officers were on duty 24/7 for the building housing the Erich Lindemann 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 business offices and the file server room. 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 staff.

We found that adequate environmental protection controls, such as smoke detectors and fire alarms, were in place in the ELMHC to help prevent damage to, or loss of, IT resources. Emergency procedures were

posted in the administrative office and, according to DMH and ELMHC 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 above floor level on racks to prevent water damage and water detection devices were located within the server room. A fire suppression system was installed in the server room and a hand-held fire extinguisher was available for employee use.

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 ELMHC employees terminate employment or incur a change in job requirements. A security officer was designated; policies and procedures were documented; and ELMHC 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 ELMHC employees listed on a current personnel roster. 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 ELMHC'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 June 2008, could be relied upon as a current, accurate, complete, and valid record of computer equipment installed at ELMHC. 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 ELMHC staff responsible for inventory were aware of the requirements and that ELMHC reported one occurrence of missing or stolen computer equipment during the audit period. Regarding the three notebook computers assigned to managers, we found that ELMHC maintained appropriate controls regarding the assignment of notebook computers to managers, such as supervisory approvals.

Our audit revealed that DMH understood the need for business continuity planning and had made efforts to develop a comprehensive plan. We determined that although DMH had developed important control practices in a variety of documents, an approved, comprehensive, and tested business continuity plan that addressed the loss of IT systems and processing capabilities and delineated specific recovery strategies for

ELMHC had not been completed. We acknowledge that DMH had designated its mission-critical systems, noted significant risks to the loss of its automated systems, and had documented additional controls over off-site storage of backup media. Also, according to DMH management, a draft business continuity plan had been documented.

AUDIT RESULTS

Business Continuity Planning

Our audit disclosed that although the Department of Mental Health (DMH) had documented certain important control practices regarding business continuity planning in various documents, none of the written documentation provided sufficient recovery strategies or identified resources required to restore normal business operations for mission-critical and essential functions in a timely manner should automated systems be unavailable for an extended period at the Erich Lindemann Mental Health Center (ELMHC). For example, we determined that the "Pandemic Influenza, Continuity of Operations Plan (COOP) for the Department of Mental Health" as of August 10, 2006," "DMH Erich Lindemann Mental Health Center Emergency Preparedness Plan" as of February 17, 2009, and the "DMH Applied Information Technology Emergency Response and Support Plan" as of December 2007, addressed significant elements fundamental to business continuity planning, such as emergency/evacuation procedures, alternate processing sites, a listing of essential business functions, designation of the ELMHC's mission-critical systems, certain notification procedures, contact information, and information regarding backup procedures.

The "DMH's IT Disaster Recovery and Business Continuity Approach," as of December 2008, presented a framework, including concepts, such as risk assessments and threats to IT operations for a business continuity plan. However, the stated controls in these documents needed further development or enhancement to constitute a comprehensive disaster recovery and business continuity plan. Furthermore, we found that, with the exception of the "DMH Erich Lindemann Mental Health Center Emergency Preparedness Plan," control practices were not tailored to the specific requirements of the ELMHC. We determined that although backup procedures for magnetic media residing on the workstations and file servers at the administrative office were adequate, environmental protection controls regarding on-site storage of magnetic media need improvement.

We acknowledge that DMH had made efforts to strengthen control practices regarding disaster recovery and business continuity planning. At the close of the audit, we found that DMH had designated mission-critical systems, noted significant risks to the loss of its automated systems, and had documented additional controls over its off-site storage of backup media. According to DMH management, a draft business continuity plan had been documented.

Depending on the nature and extent of a loss of IT systems or processing, ELMHC 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 the needs of the Lindemann.

DMH, Metro Boston Area Office (MBAO), and ELMHC need to further collaborate to strengthen business continuity-related control practices, as follows:

- Perform a criticality assessment and risk analysis;
- Document all potential disaster scenarios and instructions to follow for each specific event;
- Document detailed procedures for establishing and relocating personnel to an alternate site, including designated staff for each site, supplies, and equipment;
- Maintain a contact list delineating 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; and
- Develop user area plans documenting procedures to follow for each business unit should automated systems be unavailable so that business activities can continue.

The objective of business continuity planning is to help ensure the recovery and 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.

For those IT services provided by IT entities, the Lindemann needs to obtain sufficient assurance that appropriate backup plans are in place. If there is a possibility that the IT services upon which the

Lindemann's mission-critical functions rely may not be recovered in a timely manner, ELMHC should develop contingency plans to address the extended loss of those IT services.

Recommendation

We recommend that to strengthen business continuity planning, ELMHC, in conjunction with DMH's Central Office and the Metro Boston Area Office, should:

- Identify disaster recovery and business continuity planning criteria, including recovery strategies, plans, procedures, and support services that ELMHC would need to implement to resume operations in a timely manner.
- Document contingency and user area plans for automated systems not under Lindemann's control, such as the Mental Health Information System installed at the Massachusetts Information Technology Center.
- Perform an enterprise-based risk analysis and criticality assessment to ensure that all functional areas and business processes are supported by technology at the Lindemann.
- Review the list of disaster scenarios regarding the loss of IT systems that would impact ELMHC operations and business functions, clarify the relative importance of business functions and the potential impact of a loss of IT processing support from each activity, and document recovery and business continuity strategies for each of the disaster scenarios identified.
- Ensure that required services and support from all mission-critical and essential business partners and third-party providers are documented and the scope of services and recovery actions to be taken are understood by appropriate staff.
- Establish targets for acceptable time periods by which mission-critical IT operations and business functions need to be recovered and include the time frames in the business continuity plan.
- Document procedures for establishing alternate processing sites, as needed, and ensure that appropriate resources are available at the sites.
- Gain an understanding of Lindemann's role and responsibility in the testing of a business continuity plan, participate in the review and evaluation of results, and obtain assurance that corrective action is taken.
- 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, MBAO, and ELMHC officials, senior management, IT staff, and ITD administrators and staff.
- Train appropriate ELMHC staff in the execution of the business continuity and contingency plans under emergency conditions. Ensure that all key management and staff have adequate skill and knowledge to carry out all tasks and activities outlined in recovery and business continuity plans.
- Strengthen environmental protection controls over on-site copies of magnetic media stored at the administrative office.

Auditee's Response

DMH has focused its Business Continuity Planning under the Office of Emergency Preparedness. Continuity of Operations (Coop) Plans, Pandemic Planning, IT Service Continuity Management, Site Business Continuity Planning are all efforts that are under review and assessment. In support of those efforts, DMH Applied Information Technology (AIT) has undertaken the formation of an Information Technology Infrastructure Library (ITIL) supported approach of emergency planning in the form of an Information Technology Service Continuity Management Plan. ITIL are a series of books and training manuals/classes that outline and explain the practices that are the most beneficial to IT service (usually manager focused). It is a business standard that Executive Office of Health and Human Services (EOHHS) and the Executive Office for Administration and Finance's (EOAF) Information Technology Division (ITD) have embraced. The plans for the implementation of that effort were shared with the Auditors. Since the audit began, progress has been made and a draft is under internal review. Further steps scheduled for the next few months are a complete criticality assessment for all business applications supported by DMH AIT and a comprehensive test plan. Once those tasks are complete, DMH AIT will present a draft plan for DMH Emergency Preparedness review and acceptance. Once we have passed that milestone, DMH will then share that draft with the Auditors for their further review and input if they would be willing to do so.

Auditor's Reply

We are pleased that DMH's Applied Information Technology Division has continued to improve control practices regarding business continuity planning. We acknowledge DMH management's decision to select a structured approach, such as the Information Technology Infrastructure Library, to help develop an Information Technology Service Continuity Management Plan. In addition, we concur with the decision to perform a criticality assessment for DMH business applications and to develop a comprehensive test plan.

We reiterate that the Erich Lindemann Mental Health Center should work in conjunction with DMH Central Office and the Metro Boston Area Office to develop appropriate business continuity planning strategies and documented plans. We will review the draft business continuity plan and associated documents, such as the criticality assessment and test plan, when they are made available by DMH and we will evaluate business continuity planning at our next audit.

Department of Mental Health
Erich Lindemann Mental Health Center
Summary of Internal Control Practices
as of February 28, 2009

Pg Ref	Control Area	Control Objective	Control Activities	Status of Control	Documented Controls	Adequacy of Documentation
10	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, DMH police officers on duty	In Effect	Yes	Adequate
10	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	Adequate
11	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 authorization, activation, and deactivation of logon IDs and passwords; users required to sign formal security statement.	In Effect	Yes	Adequate
11	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
Erich Lindemann Mental Health Center
Summary of Internal Control Practices
as of February 28, 2009

Pg Ref	Control Area	Control Objective	Control Activities	Status of Control	Documented Controls	Adequacy of Documentation
11, 13	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, 13	On-site storage for backup copies generated at ELMHC	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	Adequate
10, 13	Off-site storage for backup copies generated at ELMHC	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.	In Effect	Yes	Adequate

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.