`

Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

Official Audit Report – Issued September 30, 2011

University of Massachusetts Medical School's Data Center Relocation

For the period July 1, 2008 through August 31, 2010

TABLE OF CONTENTS/EXECUTIVE SUMMARY

The University of Massachusetts Medical School (UMMS), which was established in 1962, is an institution of higher education offering three graduate schools: the School of Medicine, the Graduate School of Biomedical Sciences, and the Graduate School of Nursing. The UMMS main campus is located in Worcester on a 63-acre campus that is shared with clinical partner UMass Memorial Health Care, and a secondary campus is located in Shrewsbury. UMMS, which is staffed by approximately 6,200 employees, was created under Chapter 15A of the Massachusetts General Laws with the purpose of providing, fostering, and supporting public higher education of the highest quality within the Commonwealth.

In accordance with Chapter 11, Section 12, of the General Laws, we performed an IT audit regarding the relocation of UMMS's data center for the period July 1, 2008 through August 31, 2010. Our audit scope included an evaluation of strategic and project planning for the new data center; the process of contracting with the vendors involved with the planning, design, construction, and relocation of the new data center; and controls over physical security, environmental protection, and disaster recovery and business continuity planning.

Based on our examination, we have concluded that, except as noted in the Audit Results section of this report, for the period July 1, 2008 through August 31, 2010, adequate internal controls were in place to provide reasonable assurance that IT control objectives would be met regarding IT organization and management, on-site and off-site storage of back-up copies of magnetic tape media, and IT-related service contracts associated with the data center relocation. Regarding the new data center, adequate controls were in place for physical security, environmental protection, and the capacity to support continuous system availability at that site. In addition, the new facility has the capability for expansion and could host additional servers to support application systems and other IT capabilities. However, our audit determined that improvements were necessary in UMMS's disaster recovery and business continuity planning and in its IT strategic planning.

Our audit found that UMMS needed to strengthen and document strategies for recovering IT capabilities. Specifically, UMMS did not have a tested and approved business continuity plan containing disaster recovery strategies for all IT functions as of the end of our audit period. UMMS's continuity-of-operations plans for certain departments, its internal control plan, and its Emergency Operations Plan contained multiple elements of disaster recovery and business continuity planning, and there is a reasonable likelihood that UMMS would be able to resume mission-critical business operations should a disaster render the IT systems at the data center inoperable. Nevertheless, UMMS could experience delays in recovering IT operations because its disaster recovery and business continuity plans need to be more comprehensive and detailed.

2. INFORMATION TECHNOLOGY STRATEGIC PLANNING IMPROVEMENTS NEEDED 11

Our audit indicated that existing strategic planning and project management procedures were not sufficiently detailed to sustain UMMS's convergence of business objectives and IT alignment. A goal of UMMS regarding IT governance should be to align all IT projects with research requirements and business strategic plans; however, the process UMMS used to facilitate this alignment across all departments lacks formal authority and supporting policies and procedures necessary to be effective. The lack of a comprehensive, long-term IT-specific strategic plan increases the risk that major system developments, IT acquisitions, or IT-related initiatives would not achieve management or user expectations and could result in time and budget overruns. The purpose of a comprehensive IT strategic plan is to provide a formalized, entity-tailored approach for developing and managing IT-related projects that support UMMS's mission and business objectives. UMMS should continue the development of a formal IT strategic planning process that ensures the alignment of all IT projects to business strategy and operations and strengthens overall IT governance.

INTRODUCTION

Background

The University of Massachusetts Medical School (UMMS), which was established in 1962, is an institution of higher education offering three graduate schools: the School of Medicine, the Graduate School of Biomedical Sciences, and the Graduate School of Nursing. The UMMS main campus is located in Worcester on a 63-acre campus that is shared with clinical partner UMass Memorial Health Care, and a secondary campus is located in Shrewsbury. UMMS, which is staffed by approximately 6,200 employees, was created under Chapter 15A of the Massachusetts General Laws with the purpose of providing, fostering, and supporting public higher education of the highest quality within the Commonwealth.

UMMS's primary mission is to advance the health and well-being of people through pioneering advances in education, research, and health care delivery. UMMS's educational mission is to provide affordable, high-quality medical education to qualified residents of the Commonwealth. With that primary objective, UMMS's educational mission has expanded to include residency and fellowship training, graduate education in nursing and the biomedical sciences, training in allied health professions, and continuing education for health care practitioners.

UMMS's administrative operations and academic mission are supported by computer services that are provided by UMMS's Information Services (IS) operations, whose primary responsibility is to support UMMS in achieving its mission, strategic goals, and objectives by ensuring the availability of secure and reliable application systems and information technology (IT) capabilities. IS provides assistance and guidance to administrative staff, researchers, faculty, and students regarding the use of IT resources, including network resources, Internet portal support, and web-hosting services. IS also evaluates emerging trends and technologies and assesses the potential operational and security impact of changes in technology at UMMS.

IS operations are composed of five departments: Product Support and Technology, Business Relations and Consulting, Telecom Services, Enterprise Network Services, and Academic and Research Computing. At the time of our audit, IS consisted of 163 full-time employees headed by a Chief Information Officer (CIO) who reports directly to the Vice Chancellor of Administration and

Finance. Each of the five departments is under the direction of an Associate Chief Information Officer who reports to the CIO.

UMMS's original legacy data center, which was located at the Worcester campus, was constructed in 1979 with 1,100 square feet of space. In 1989, the data center was expanded by 3,300 square feet adjacent to the original computer room. From 2006 to 2008, the data center was further enhanced by adding uninterrupted power supply capacity, additional cooling capacity, and automatic transfer switching capabilities. Despite these renovations, numerous weaknesses in environmental conditions, reliability, and technology still existed in the data center. In addition, weaknesses in the data center included limited space and a lack of capacity to meet increasing processing demands. Because of these weaknesses, in March 2008 UMMS senior management decided to develop a new data center at the Shrewsbury location in order to improve IT security, reliability, and system availability. As of November 2010, the Worcester legacy data center had been completely shut down and no longer housed any of UMMS's application systems.

At the conclusion of our audit, IT operations were supported by 297 file servers configured in a virtualized environment located in the new data center. Virtualization capabilities allow UMMS to run various application systems in separate, isolated sections within single servers. Each isolated section runs its own application that can be moved or copied from one server to another, permitting processing and communications activity to be distributed evenly across the computer network so that servers are not overwhelmed or underutilized. In addition, the UMMS IT infrastructure included 3,892 workstations and 880 laptop computers that are distributed to departments throughout UMMS for faculty, administrators, and staff and are configured to provide access to IT capabilities through UMMS's network. UMMS is also connected through a wide area network to the Commonwealth Information Technology Division's primary data center located in Chelsea, providing access to the web-based Human Resources/Compensation Management System and the Massachusetts Management Accounting and Reporting System.

UMMS utilizes a total of 18 essential systems to support mission-critical business functions that are housed at the new data center. UMMS has seven mission-critical infrastructure-related systems: Legato Backup, Sybari Antigen, Remote Authentication Dial-In User Service, VMware, Checkpoint Firewall, Checkpoint Firewall Management Console, and network file and print services. UMMS also utilizes Microsoft Exchange for email purposes, in addition to five other mission-critical telecom-related systems: Aspect, Blackberry Enterprise Servers, Cisco Call Manager, Digital Notification Announcer, and Ivize. Additionally, UMMS utilizes five other mission-critical and essential systems: PeopleSoft, Endeavour, HEAT Business Process Automation Module, R-Drive, and WebCT.

Audit Scope, Objectives, and Methodology

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an IT audit regarding the relocation of UMMS's data center for the period July 1, 2008 through August 31, 2010. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our primary audit objective was to determine whether UMMS's IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that control objectives would be met to support UMMS's project planning and relocation to the new data center. The audit included an assessment of the adequacy and effectiveness of controls in place to plan, design, and oversee the construction, purchase, and transfer of equipment; relocation to the new data center; and protection of the application systems and the supporting IT infrastructure contained within the new data center.

To determine the scope of the audit, we performed pre-audit work regarding UMMS's overall mission and IT environment. The pre-audit work included interviews with senior management and a review of documentation pertaining to policies, procedures, and internal controls related to the planning, design, construction, cost, and relocation of the data center. We also reviewed third-party service provider contracts related to the relocation of the data center and analyzed policies and procedures used to help ensure that contracts are initiated, managed, and processed in compliance with state regulations. To obtain an understanding of internal control requirements, we reviewed UMMS's mission, business objectives, and the business case for the planning and construction of the new data center. We conducted a high-level risk analysis regarding the data center relocation and assessed the appropriateness of internal controls and project management procedures for physical security, environmental protection, system access security, inventory control over IT equipment, business continuity planning, and on-site and off-site storage of back-up media relevant to the new data center. Upon completion of our pre-audit work, we determined the scope and objectives of the audit and developed our audit strategy.

Our audit scope included an evaluation of strategic and project planning for the new data center; the process of contracting with the vendors involved with the planning, design, construction, and relocation of the new data center; and the controls regarding physical security, environmental protection, and disaster recovery and business continuity planning.

We reviewed physical security controls for the data center, including doorways, card key locks, and monitoring functions. We also reviewed the physical layout of the data center. Additionally, our audit scope included a review of controls over environmental risks, such as fire and heat, power surges and outages, water damage, and man-made threats. To aid in the evaluation of the environmental controls, we referred to ITD-SEC 1.2, the Enterprise Information Security Policy from the Commonwealth's Information Technology Division (ITD); Control Objectives for Information Technology 4.1 (CobiT 4.1) Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance; and ISO/IEC 27002, an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). In addition, we determined whether documented policies and procedures regarding logical access security were in existence.

Our audit objective regarding UMMS's IT organization and management was to determine whether IT-related roles and responsibilities for UMMS's staff providing oversight regarding the planning, construction, and relocation of the data center were clearly defined; points of accountability were established; appropriate organizational controls, such as documented procedures and strategic plans, were in place and in effect; and IT-related policies and procedures adequately addressed the areas under our review. We determined whether a documented planning process was in place from which IT strategic and tactical plans would be developed to help direct the implementation and use of IT to fulfill UMMS's mission and goals.

We evaluated whether UMMS had implemented adequate controls regarding contract management to provide reasonable assurance that IT-related contract monitoring and evaluation were being performed. We verified whether contractual relationships with third-party service providers were in writing, whether the contract agreements sufficiently detailed services or deliverables to be provided, and were properly signed and dated.

With respect to the operational availability and application systems relocated to the new facility, we determined whether disaster recovery and business continuity strategies provided reasonable assurance that mission-critical and essential IT capabilities could be regained within an acceptable period of time should IT resources be rendered inoperable or inaccessible. In addition, we determined whether adequate control procedures were in place and in effect for the generation and on-site and off-site storage of back-up copies of magnetic media to support system and data recovery objectives.

We determined whether adequate physical security controls were in place to provide reasonable assurance that access to the new data center would be limited to only authorized personnel. Additionally, we determined whether sufficient environmental protection was provided to the data center to prevent or detect damage or loss of IT-related equipment and media. Our audit objective regarding internal controls over financial resources was to determine whether UMMS had procedures in place to provide for the accurate and complete accounting of costs associated with the planning, construction, relocation, and maintenance of the new data center.

We evaluated the degree to which UMMS had a documented business case to support the relocation of the data center and whether a documented project plan had been developed. We determined whether appropriate budget controls had been established to provide cost tracking for the project. We determined whether an IT strategic plan existed and included the relocation of the data center and assessed whether IT strategic planning was aligned with UMMS's operational strategic planning.

We assessed the adequacy of disaster recovery and business continuity planning at UMMS regarding application systems relocated to the new facility. We reviewed the level of planning and the procedures to be followed to resume computer operations in the event that the automated systems were rendered inoperable or inaccessible at UMMS's new data center. We interviewed UMMS management to determine whether the criticality of application systems had been assessed, a risk analysis of computer operations had been performed, and documented formal business continuity planning was in place and tested. In addition, we reviewed the status of management's efforts to designate an alternate processing site to be used should the new facility be damaged or become inaccessible.

We determined whether UMMS had developed an enterprise risk management framework to identify threats to the data center, assess the risk or impact presented by the threats, determine the feasibility of implementing controls to address the risks, implement appropriate controls, and reassess the risks periodically or upon major changes to the business or IT environment. We interviewed UMMS senior management from the President's Office, IS, and the Facilities Management; conducted data center walkthroughs; and reviewed related documentation.

Based on our examination, we have concluded that, except as noted in the Audit Results section of this report, for the period July 1, 2008 through August 31, 2010, adequate internal controls were in place to provide reasonable assurance that IT control objectives would be met regarding IT organization and management, on-site and off-site storage of back-up copies of magnetic tape media, and IT-related service contracts associated with the data center expansion. Regarding the new data center, adequate controls were in place for physical security, environmental protection, and the capacity to support continuous system availability at that site. In addition, the new facility has the capability for expansion and could host additional servers to support application systems and other IT capabilities. However, our audit determined that improvements were necessary in UMMS's disaster recovery and business continuity planning and in its IT strategic planning.

AUDIT RESULTS

1. DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING IMPROVEMENTS NEEDED

Our audit found that the University of Massachusetts Medical School (UMMS) needed to strengthen and document strategies for recovering IT capabilities. Specifically, UMMS did not have a tested and approved business continuity plan containing disaster recovery strategies for all IT functions as of the end of our audit period. UMMS's continuity-of-operations plans for certain departments, its internal control plan, and its Emergency Operations Plan contained multiple elements of disaster recovery and business continuity planning, and there is a reasonable likelihood that UMMS would be able to resume mission-critical business operations should a disaster render the IT systems at the data center inoperable. Nevertheless, UMMS could experience delays in recovering IT operations because its disaster recovery and business continuity plans need to be more comprehensive and detailed.

Despite the various elements of business continuity strategies that existed and the successful restoration of all application systems at the time of the failure, UMMS did not have formally documented and comprehensive business continuity and disaster recovery plans to provide adequate assurance of the timely restoration of mission-critical and essential business functions should information technology (IT) systems be rendered inoperable or inaccessible. Sufficiently detailed and documented formal recovery and contingency plans would help ensure that processing could be regained for mission-critical and essential IT systems within an acceptable period of time should a catastrophic disaster occur. The absence of a formally documented recovery and contingency plan addressing disaster recovery places at risk the ability to resume computer-related operations to support business operations in an adequate and timely manner should a major emergency occur. IT business continuity planning consists of a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of mission-critical and essential IT systems and operations and access to online information.

Although UMMS had identified the need for an alternate processing site, we determined that UMMS had not identified an off-site location for back-up computer operations or the relocation of staff. We also found that UMMS had an Emergency Operations Plan that provided high-level response procedures for UMMS personnel in the event of a potential threat to staff or students at the Shrewsbury facility. However, this plan did not clearly integrate IT operations into the overall emergency response strategy. While management had informally assessed the relative criticality of their computing systems and developed various policies, a formal criticality assessment and business impact analysis of all UMMS systems, applications, and user departments had not been performed.

At the time of our audit, only 23 of 96 sub-department continuity of operations plans had been developed to address the recovery of business operations supported by UMMS's Information Services (IS) operations should a disaster occur. We noted that UMMS's Emergency Operations Plan includes a number of various risks to the health and safety of personnel at UMMS. Given its purpose and current content, the plan should not be considered an IT business continuity or contingency plan. Although there is a strong understanding that disaster recovery capabilities must be in place, a thorough risk analysis of IT capabilities in line with business operations would identify the relevant threats that could significantly impair or render IT systems inoperable or inaccessible, the likelihood of the threats, and expected frequency of occurrence for each disaster scenario. We noted that the eight completed department-specific continuity of operations plans could be strengthened by further documenting the necessary tasks and responsibilities for all relevant UMMS personnel to address UMMS's business objectives under various disaster scenarios. Documentation of key processes and activities relating to business objectives helps to provide clear guidelines regarding implementation and expected results.

Business continuity plans should be tested to validate their viability and to reduce both the risk of errors and omissions and the time needed to restore computer operations. In addition, an effective recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios that could render IT systems inoperable. Specifically, the plan should identify how essential services would be provided for each scenario without the full use of data processing facilities, and the manner and order in which processing resources would be restored or replaced. Furthermore, the plan should identify the policies and procedures to be followed, including details of the logical order for restoring critical data processing functions, either at the original site or at an alternate site. The plan should also identify and specifically detail the tasks and responsibilities necessary to transfer and safeguard back-up magnetic copies of data files, program software, and system documentation from off-site storage to the site being used for restoration efforts.

Sound management practices as well as industry and government standards support the need for comprehensive and effective back-up procedures and business continuity plans for organizations that depend on technology for information processing. Contingency planning should be viewed as a process to be incorporated within an organization, rather than as a project completed upon the drafting of a formal documented plan. Since the criticality of systems may change, a process should be in place that will identify a change in criticality and amend the contingency plans accordingly. System modifications to IT equipment configurations and user requirements should be assessed in terms of their impact on existing business continuity plans.

Without a comprehensive and well-documented formal business continuity and disaster recovery strategy for all IS functions and operations, UMMS may be unable to recover mission-critical and essential business activities in an acceptable and timely manner.

Recommendation

We recommend that UMMS strengthen its disaster recovery and business continuity planning processes by:

- Developing and maintaining appropriate recovery strategies to regain mission-critical and essential processing within acceptable time periods.

- Ensuring that a detailed business impact analysis is performed for functional areas to confirm the impact of a loss of IT systems and the point at which IT capabilities need to be restored.

- Encouraging a more collaborative effort among IS and business process owners to ensure that continuity plans are developed that take into account business and IT dependencies.

- Documenting a more comprehensive disaster recovery plan that includes recovery strategies with respect to various disaster scenarios and specific information needed by recovery teams and business areas to effectively and efficiently recover mission-critical and essential IT and business operations within required time frames.

- Documenting contingencies and the steps to be followed by various user groups to continue business operations to the extent possible should IT capabilities or resources be rendered unavailable. All such recovery and continuity planning documents should be available in electronic and hard copy form, and should be stored off-site in secure, accessible locations.

- Annually testing the viability of its alternate processing site, and documenting and evaluating the scope and results of the tests performed.

- Specifying the assigned responsibilities and points of accountability for maintaining and implementing all recovery and continuity planning documents and identifying who is to be trained in the implementation and execution of the plans under all emergency conditions.

- Training UMMS personnel in their responsibilities for recovering business operations in the event of an emergency or disaster, including the instruction of office staff on manual procedures to be used to the extent possible in the event that processing is delayed for an extended period.

- Establishing procedures to ensure that the criticality of systems is evaluated and that business continuity requirements are assessed annually or upon major changes to user requirements or IT systems.

- Distributing the completed business continuity plans to all appropriate staff members in both hard copy and electronic media.

Auditee's Response:

The Medical School opened a state of the art Data Center in 2010 and relocated all systems and operations from the 30-year–old, legacy data center on the Worcester campus. The new Data Center was constructed with multiple redundant air handling, monitored electrical systems and back-up generators which mitigate the risk of unscheduled outages from HVAC and electrical failures. The overall design of the data center includes provision for a minimum of 10 years growth with a design that allows for future expansion beyond the current footprint.

UMMS Information Services recognizes the need for the development of a formal Disaster Recovery Plan (DRP) as well as completing the UMMS Business Continuity Plan (BCP). The Medical School does not currently have an arrangement for a site for alternate IT operations.

In April 2011, the School contracted with EMC to lead a collaborative effort with UMMS Information Services to strengthen and expand our existing DRP program. As part of the effort with EMC, we will document strategy options with budgetary considerations for senior management review and approval. The engagement deliverables consist of the following:

- *Perform full application analysis, business impact assessment for UMass systems*
- *Assess and document business continuity capabilities*
- *Document 2 to 3 DR strategies/options, including high level architecture and budgetary considerations*
- *Create recommendations for mitigating DR program gaps with solution roadmap*

Additionally, the UMMS Emergency Operations Committee has been actively developing [a] Continuity of Operations Plan (COOP) for Information Services (IS). This plan, along with the IS BCP and DRP documents are expected to be completed and approved by November 2011. These COOP plans are complimentary to the BCP and incorporate important aspects of business continuity process including business impact analysis and definition of business application priorities for UMMS departments. We also recently initiated a tabletop exercise, in cooperation with the UMMS Emergency Management Committee to examine and further validate our disaster recovery strategy and evaluate the improvements that have already been made.

> *Finally, in support of the business operations surrounding the new data center and the prioritization of enhancing planning procedures, a Data Center Manager was hired in June 2010. A key responsibility for this Manager has been to work with the UMMS Emergency Operations Committee and other departments such as Facilities, to drive IS DRP and BCP processes and procedures on an ongoing basis.*

2. INFORMATION TECHNOLOGY STRATEGIC PLANNING IMPROVEMENTS NEEDED

Our audit indicated that although UMMS has a clear understanding of its mission and business objectives, its IT strategic planning and project management procedures were not sufficiently detailed to ensure the alignment of IT and business strategic planning. As a result, there is inadequate assurance that UMMS's IT investment fully supports its business objectives and that its IT enabling capacity is maximized. IT strategic planning also helps ensure that there is a coordinated effort to achieve relevant internal control objectives for UMMS's new data center and future IT-related projects.

Although there is awareness that IT infrastructure management is important, IT strategic planning was handled on an informal basis. For example, it is clear that detailed planning was performed regarding the new data center, as demonstrated by the relocation of computer equipment and systems being accomplished within relatively short time periods and without incident. However, the implementation of a formal IT planning process, in concert with performance metrics, would enhance project management documentation and UMMS's ability to evaluate IT value delivery. UMMS did not have a formal documented process in place at the time of our audit to make adequate decisions about the appropriateness, cost-effectiveness, and necessity of implementing data center controls.

UMMS needs to document procedures that ensure the alignment of all IT projects with business functions and prioritize all IT initiatives. IS senior management recognized the need for IT strategic planning; however, at the time of our audit, IT strategic planning at UMMS was performed on an as-needed basis in response to a specific business requirement or weakness identified in the infrastructure. UMMS's IT strategic plan should be derived from UMMS's underlying business model and IT strategic goals and objectives, which should be based on UMMS's mission, vision, and value statements. Working in conjunction with the business model, the IT strategic plan should reflect how technology is being utilized to meet current and future business objectives.

The role of IT governance and an IT strategic plan alignment with UMMS departments is imperative to maximize overall business success. Implementation of an integrated IT strategic plan that aligns with UMMS business planning and strategy is the fundamental key to IT governance supporting UMMS's business growth and stability. Moreover, focus on strategic IT alignment results in the creation of cross-functional teams with participation from executive-level leadership. These teams help ensure the alignment of business and IT strategies and the proper allocation of IT resources. Concerted efforts on formal strategic planning and performance management can assist UMMS in keeping pace with the technology curve while achieving the highest return possible on IT-related initiatives. Additionally, UMMS would position itself to better support internal users and focus resources on the right investments and projects.

Recommendation

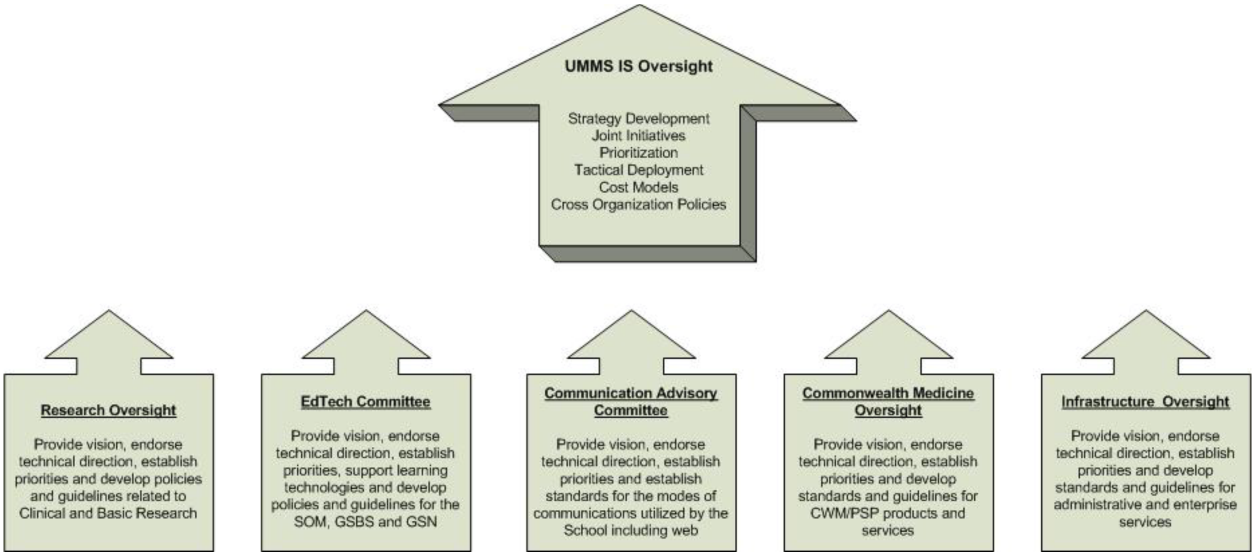
We recommend that IS adopt an IT strategic planning process in which IT strategic plans are developed in alignment with UMMS's organizational business strategy. This approach should support strategic planning to better align IT activities with the operational requirements of UMMS's departments. UMMS management should incorporate business groups in the planning process, integrate the process with UMMS's planning calendar, and update plans frequently enough to keep pace with demand. UMMS should, in collaboration with relevant departments, develop an IT strategic plan that defines how IT goals will contribute to UMMS's strategic objectives and related costs and risks. The IT strategic plan should cover investments and the operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements, and should be sufficiently detailed to allow for the definition of tactical IT plans.

There are various strategic planning processes that would allow for timely and appropriate responses to unpredicted scenarios. For example, a SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis, an extremely useful tool for the understanding of and decision-making during various situations in business and organizations, would greatly benefit UMMS. The framework of a SWOT analysis would allow for the review of IT strategies, positions, procedures, and the direction of UMMS's IT initiatives. However, medium- to long-term goals and directives for future IT-related strategy development are still a key component of a well-documented IT strategic plan.

Auditee's Response:

The Medical School previously conducted planning on an annual basis in concert with the annual budgeting process. During that annual effort, all strategic information and technology initiatives were presented to Senior Management for prioritization and budget allocation. This annual process was an integrated approach and was not separately documented as is noted above.

The Medical School Information Services has recently implemented a tightly integrated governance structure that will significantly enhance the strategic planning process and the documentation of same. That process is depicted below. We expect that this structure will facilitate a plan that integrates the numerous disciplines and competing requirements of the broad constituencies within the Medical School.


UMMS IS Oversight
Strategy Development
Joint Initiatives
Prioritization
Tactical Deployment
Cost Models
Cross Organization Policies
Research Oversight
Provide vision, endorse technical direction, establish priorities and develop policies and guidelines related to Clinical and Basic Research
EdTech Committee
Provide vision, endorse technical direction, establish priorities, support learning technologies and develop policies and guidelines for the SOM, GSBS and GSN
Communication Advisory Committee
Provide vision, endorse technical direction, establish priorities and establish standards for the modes of communications utilized by the School including web
Commonwealth Medicine Oversight
Provide vision, endorse technical direction, establish priorities and develop standards and guidelines for CWM/PSP products and services
Infrastructure Oversight
Provide vision, endorse technical direction, establish priorities and develop standards and guidelines for administrative and enterprise services

We expect this governance structure to produce more cohesive and efficient strategic plans. Project recommendations will be generated from the five (5) sub-group Oversight Committees and the strategies will be vetted across all groups prior to being submitted to the top level UMMS IS Oversight group. Any recommended strategies will be based upon a comprehensive analysis of strengths, weaknesses, opportunities and threats. The top level UMMS IS Oversight group will review and discuss the final recommendations in relation to other institution strategies before any revisions or approval.

In the past, we believe that IS has done an excellent job in delivering on strategic initiatives as evidenced by the final "product" delivered in the recent UMass Worcester data center build and migration. The final outcome satisfies and will continue to meet all of the needs for the Medical School and its partners on a long term basis. The Data Center has the required security and redundancy necessary for a world class medical education and research facility and is extremely environmentally friendly and cost efficient. While the overall plan was developed as a joint effort between IS and the Facilities department, the overall objectives were based on the collective technology needs of the campus and vetted with departments.

In 2010, the UMass Medical School enhanced its annual strategic planning process where Information Services plays a key role in the development, facilitation and delivery of enterprise based solutions to support the defined strategies. Our more integrated IS governance structure plays a key role in assuring that the institution has the required information technology deployed to support those strategies going forward for the UMass Medical School, the Medical School's partners and the UMass University System.