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

Official Audit Report – Issued April 30, 2012

IT-Related Controls at the University of Massachusetts Amherst

For the period July 1, 2009 through May 31, 2011

TABLE OF CONTENTS/EXECUTIVE SUMMARY

Chapter 15A of the Massachusetts General Laws authorizes the University of Massachusetts Amherst (UMA) to provide, foster, and support public higher education of the highest quality throughout the Commonwealth. The University of Massachusetts system, which consists of campuses in Amherst, Boston, Dartmouth, Lowell, and Worcester, was established by Chapter 75, Section 1, of the General Laws.

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, the Office of the State Auditor performed an information technology (IT) audit at UMA that covered the period July 1, 2009 through May 31, 2011. The audit scope included an examination of the IT governance at UMA and an evaluation of internal and general controls over the mission-critical SPIRE application system, including physical and environmental controls that directly affect UMA's computing operations (excluding human resources and financial applications, which are hosted and operated by the UMass President's Office in Shrewsbury). Based on our examination, we have concluded that adequate controls were in place over UMA's mission-critical SPIRE application to provide reasonable assurance that business objectives would be met. However, as reported in the Audit Results section of this report, as of May 31, 2011, UMA needed to make improvements in the areas of IT governance, IT strategic planning, and business continuity and disaster recovery planning.

Our audit disclosed that UMA's IT governance is informal and decentralized, indicating a lack of coordination among autonomous budgetary units and the Office of Information Technology (OIT), a problem that could be reduced by clearly defining UMA's IT strategy and communicating it effectively throughout the university. At the time of our audit, administrative security controls over the IT environments across each of the business units were inconsistent with regard to the management of the IT infrastructure. We noted that UMA had experienced three data breaches over a two-year period. Our audit indicated that although the breaches were handled professionally and appropriately after they were discovered, stronger IT governance and support structures would reduce the risk of such breaches and ensure the consistent application of sound IT practices.

Our audit indicated that IT strategic planning and project management procedures were not sufficiently detailed to sustain UMA's alignment of business objectives with IT-related goals. UMA's objective should be to align all IT-related projects with research requirements to business-related strategic plans. However, the process to facilitate this alignment across all of UMA's major budgetary units lacked formal designated authority, monitoring, 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, and IT-related initiatives would not achieve management or user expectations, and could result in time and budget over-runs.

3. IMPROVEMENTS NEEDED IN BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING 9

Our audit indicated that although UMA had elements of business continuity and disaster recovery planning in 109 department-specific "Continuity Action Plans," UMA had not developed formal disaster recovery plans, business continuity plans, and continuity of operations plans for the 16 critical application systems identified by OIT. As a result, UMA could experience delays in recovering IT operations in the event of a disaster. Business continuity plans should be tested to validate their viability and to reduce both the risk of errors and omissions, as well as 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 would render IT systems inoperable or inaccessible.

INTRODUCTION

Background

The University of Massachusetts Amherst (UMA) is staffed by over 5,000 employees and enrolls over 27,000 total undergraduate and graduate students. Chapter 15A of the Massachusetts General Laws authorizes UMA to provide, foster, and support public higher education of the highest quality throughout the Commonwealth. The University of Massachusetts system, which consists of campuses in Amherst, Boston, Dartmouth, Lowell, and Worcester, was established by Chapter 75, Section 1, of the General Laws.

UMA's mission is to provide an affordable and accessible high-quality education and conduct programs of research and public service. UMA's campus is supported by technology managed by the Office of Information Technology (OIT), which consists of 214 information technology (IT) positions. The primary mission of OIT is to help enable the faculty, staff, and students of UMA to meet their IT needs. At the time of our audit, UMA's operations were supported by over 1,500 file servers located in 20 data center locations. UMA utilized 16 mission-critical application systems hosted in the various data centers, including five OIT-managed applications: SPIRE, UMail, SPARK, Exchange, and the UMA website, a campus public website and communications portal. SPIRE is OIT's most critical application system and is essential to the operations of the UMA campus.

UMA is also connected through a wide area network (WAN) to the Commonwealth's 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. In addition to over 9,800 workstations, there are over 3,900 laptops that are distributed to faculty, administrators, and a limited number of students throughout UMA with access to UMA's network. The workstations are located throughout both business and faculty offices, as well as student labs.

UMA's IT network consists of seven different geographic locations to which individual building networks are connected. The seven geographic locations also have a router function that provides connectivity between the individual building networks and other critical network routers. Additionally, two of the seven geographic sites serve as routers that interconnect the seven locations, which then connect to the campus WAN routers, providing connectivity to all off-campus network resources.

SPIRE, UMA's implementation of the Oracle Corporation's PeopleSoft Campus Solutions product, provides secure web-based access to over 30,000 people associated with the campus. SPIRE supports numerous administrative functions, including student course registration, academic records, advising, admissions, financial aid, student billing, admissions prospect communications, and federal reporting on foreign students and scholars. SPIRE provides significant self-service functionality for students, admissions applicants, faculty, and staff; is the system of record for personal data for all members of the campus community; and supports numerous interfaces to other entities both on and off campus. UMA has developed major customizations of the software to provide many campus IT services, such as email, campus network access, and authentication for learning management software on campus. Another significant customization provides strong functionality for the administration of over 10,000 campus housing assignments. SPIRE, which is the official source for all academic and student data that is provided through the campus data warehouse application, is hosted in the OIT's Lederle Graduate Research Center, with a standby database in the Dubois Library. Administration, customization, and maintenance are the responsibility of the Administrative Computing Support Organization within OIT. SPIRE users receive security training at the time of the initial access request related to the Family Education Rights and Privacy Act before gaining access to the system.

Audit Scope, Objectives, and Methodology

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, the Office of the State Auditor performed an IT audit at UMA that covered the period July 1, 2009 through May 31, 2011. The audit scope included an examination of the IT governance at UMA and an evaluation of internal and general controls over the mission-critical SPIRE application system, including physical and environmental controls that directly affect UMA's computing operations (excluding human resources and financial applications, which are hosted and operated by the UMass President's Office in Shrewsbury).

We conducted this 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.

We also conducted this performance audit in accordance with the following criteria: the Massachusetts General Laws; Chapter 647 of the Acts of 1989; and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT 4.1), issued by the Information Systems Audit and Control Association in July 2007. To aid in the identification and evaluation of IT controls, we also referred to the Enterprise Information Security Policy from the Commonwealth's Information Technology Division Infosec ITD-SEC 1.2, Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, and the International Standards Organization's ISO/IEC 27002 on IT Security Management.

Our objectives were to gain and record an understanding of IT governance, IT strategic planning, IT policies and procedures, and disaster recovery and business continuity planning over UMA's computer environment, and to determine whether such activities were managed effectively. Our methodology included a review of management reports issued by external auditors, internal auditors, and consultants to identify strengths and weaknesses regarding UMA's IT environment, and the development of a profile of the SPIRE application system to aid in the assessment of overall security regarding physical protection of equipment, software, data, and monitoring of the loss of assets such as information through theft or unauthorized use.

Regarding IT governance, we evaluated whether UMA had aligned IT strategic planning with the overall organization's business strategic planning to help achieve desired benefits, IT roles and responsibilities were clearly defined and assigned, an appropriate framework of controls had been implemented, and IT risks were managed to reduce the likelihood of adverse events. We also determined whether UMA's organizational leadership, organizational structure, and processes ensure that UMA's IT sustains the organizational strategies and objectives.

Regarding the Lederle Graduate Research Center's data center that houses the SPIRE application system, our objectives were to determine whether adequate physical security controls were in place to provide reasonable assurance that access to the data center would be limited to authorized personnel only. The physical layout of the data center was also reviewed for all points of entry, and relevant physical security controls for the data center were reviewed, including doorway locks, card key locks, and monitoring functions. 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. We reviewed controls over environmental risks, such as fire and heat, power surges and outages, water damage, poor air quality, and man-made threats. In addition, we determined whether UMA maintained documented policies and procedures regarding logical access security. We performed a high-level risk analysis, including a fraud risk assessment. The risk assessment was conducted through a review of UMA's documented policies and procedures, the SPIRE application system, and interviews with UMA management.

Based on the examination, we have concluded that, except as reported in the Audit Results section of this report, adequate internal controls, policies, and procedures were in place at UMA to provide reasonable assurance that IT-related control objectives would be met for physical security and environmental protection at the data center supporting the operation of the SPIRE application system for the period July 1, 2009 through May 31, 2011.

AUDIT RESULTS

1. IMPROVEMENTS NEEDED IN INFORMATION TECHNOLOGY GOVERNANCE

Our audit at the University of Massachusetts Amherst (UMA) disclosed that although there was a strong model of information technology (IT) governance, comprised of good management practices and controls over UMA's mission-critical SPIRE application, overall IT governance throughout all major budgetary units at UMA was informal and decentralized. At the time of the audit, campus-wide IT controls were inadequate concerning organizational controls for roles and responsibilities and points of accountability.

IT governance is how management formally decides to employ IT in supervising, monitoring, and directing an organization and is vital to overall enterprise governance. IT governance consists of executive leadership and organizational structures, processes, and frameworks of control to ensure that IT sustains and extends organizational strategies and objectives. Effective IT governance would ensure that IT supports UMA's business goals, maximizes business investment in IT, and appropriately manages IT-related risks and opportunities. Weak IT governance can result in IT strategic and tactical plans not aligning with UMA's business requirements and business plans and can also lead to poor management decisions; inadequate cost determinations; uncontrolled expenditures; failed or subpar systems; lack of performance measurement; and noncompliance with laws, regulations, or contractual obligations. Exercising fundamental IT governance principles ensures that appropriate control frameworks are in place and in effect to provide assurance that operational and control objectives are met.

During our pre-audit work, it was revealed that three data breaches had occurred at UMA in a two-year period. The three breaches shed light on the need to strengthen IT governance, as well as the critical importance of data security and protection of personal information on all servers at UMA (a total of 16 mission-critical application systems could be affected). Our audit indicated that although the breaches were handled professionally and appropriately after they had been discovered, stronger IT governance would help ensure that a consistent framework for data management would be in place within IT operations across all administrative functions. Not only are users placed at risk as a result of the loss of personal information, data breaches can cost organizations millions of dollars to remedy. Higher education contains data-rich IT environments that could be highly vulnerable to data breaches absent appropriate IT governance controls. The implementation of a formal campus-wide supervising and monitoring program for the IT environment, with a focus on business department missions and objectives, would help minimize IT-related risks and optimize resource value. Implementation of enterprise-based IT security and incident response policies and procedures across decentralized IT environments can help reduce the risk and impact of the occurrence of data breaches.

If strategic and operational decision-making is not formalized with input from business management and IT, then the benefits of IT governance may be at risk. Effective IT governance would require that the UMA Office of Information Technology's (OIT) senior management collaborate with executive staff across the Amherst campus. If OIT has the sole responsibility for creating, approving, prioritizing, and executing IT-related plans, other key stakeholders are excluded and the risk of IT failures increases. IT decisions must be guided by broad-based business knowledge, not just technology expertise.

Recommendation

IT governance at UMA needs to be strengthened across the campus to address critical factors that are key to IT governance success, such as exercising change control management, prioritizing projects, managing IT risk, aligning business and IT objectives, and identifying performance measures. UMA should improve its IT governance by:

- Implementing sound IT governance practices and structures to inform, direct, manage, and monitor activities toward the achievement of UMA's business objectives, as demonstrated by the OIT's strong controls over SPIRE.
- Establishing, through the OIT, a general monitoring framework and approach to define the scope, methodology, and process to be followed by all data centers and application owners for developing adequately aligned IT and business strategies, measuring IT's solution and service delivery, and monitoring IT's contribution and value to UMA.
- Integrating the general monitoring framework with an overall UMA performance management structure. Implementing IT governance at UMA will optimize performance and security, satisfy rapidly evolving regulations, and proactively reduce legal exposure (i.e., occurrence and impact of data breaches). An intra-departmental initiative involving chancellors, board-level executives, senior management, end-user groups, and other stakeholders whose success depends upon IT assets meeting strategic objectives and aggressive performance and compliance obligations would greatly benefit UMA.

- Developing and issuing updated IT governance policies addressing ownership of IT governance, a strategic planning framework for alignment of IT strategy with UMA business strategy, performance measurement, and management of IT risks and resources.

- Ensuring that the following best practices are part of its proposed IT governance model: IT investments should align with UMA's objectives and goals, IT-related projects should align with business values, IT risks and resources should properly be identified and managed, and IT performance should be measured and reported.

- Developing IT governance risk and compliance competencies, practices, and capabilities.

Auditee's Response

The University of Massachusetts Amherst has been working to develop a formal campus-wide Information Technology governance model and process. The first meeting of the Administrative Information Technology Coordinating Council was held in July 2011. This group, appointed by Executive Management from the respective campus business units, forms an inter-departmental effort that will continue to meet on at least a quarterly basis. The agenda will be driven by topics concerning governance, IT decision making, strategic and tactical campus needs, and budget impact of decisions. Participants in this group span the breadth of campus business units and serve to propagate best practices amongst the various campus business units with information technology responsibilities.

The campus is also in the early stages of implementing an Academic and Instructional Technology Coordinating Council to focus on issues that pertain directly to academic and instructional needs of the campus. We anticipate the first meeting of this council to occur during the spring semester 2012. This group will similarly meet on at least a quarterly basis.

Between these two councils we have broad representation of the various campus administrative and academic units on Information Technology decision-making.

We will use this group to develop formal policies and procedures. We will apply the lessons learned from our many years of formal governance deployed with the campus Student Information System (SPIRE) and look to use aspects of that as a model for other systems.

To address the risk assessment and management recommendations, the campus has instituted a formal Committee on Enterprise Risk Management (CERM). The charge of the CERM committee is to understand and manage risk on a campus wide basis. CERM includes participation from all campus units, including Information Technology, and will be an ongoing component of campus-wide risk management.

2. IMPROVEMENTS NEEDED IN INFORMATION TECHNOLOGY STRATEGIC PLANNING

Our audit indicated that although UMA had a clear understanding of its mission and business objectives, IT strategic planning and project management procedures across UMA were not sufficiently detailed to sustain the alignment of IT initiatives and goals with business department objectives. As a primary objective of IT governance, alignment of IT and business strategic planning within all major budgetary units across the campus ensures that IT investment fully supports business objectives and that IT's enabling capacity is maximized.

In addition to addressing all IT functions, IT strategic planning would also help ensure that there is a coordinated effort to achieve relevant internal control objectives for the new data center and future IT-related projects. The implementation of a formal IT planning process, in concert with performance metrics, would enhance project management documentation and UMA's ability to evaluate IT value delivery. UMA did not have a formal documented process in place at the time of the audit to make adequate decisions about the appropriateness, cost-effectiveness, and necessity of implementing data center controls.

UMA needs to document policies and procedures that ensure the alignment of all IT-related projects with business functions and provide a basis for prioritizing IT initiatives. UMA's IT strategic plan should be derived from UMA's underlying business model and IT strategic goals and objectives, which should be based on UMA's mission, vision, and value statements. Working in conjunction with the business model, the IT strategic plan should reflect how technology is utilized to meet current and future business objectives. There are various strategic planning processes that would allow for timely and appropriate responses to unpredicted scenarios. For example, an analysis of strengths, weaknesses, opportunities, and threats (SWOT), an extremely useful tool for the understanding of and decision-making during various situations in business and organizations, would greatly benefit UMA.

The role of IT governance and an IT strategic plan alignment with UMA budgetary units is imperative to maximize overall business success. Implementation of an integrated IT strategic plan that aligns with UMA business planning and strategy ensures IT governance supports UMA'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 the business and IT strategies and proper allocation of IT resources.

Recommendation

UMA should improve its IT strategic planning by:

- Adopting a generally accepted IT strategic planning process whereby IT strategic plans are developed in alignment with an organizational business strategy. This approach should support strategic planning to better align IT activities with the operational requirements of UMA's major budgetary units. UMA management should incorporate business groups in the planning process, integrating the process with UMA's planning calendar and refreshing plans frequently enough to keep pace with changes at UMA.

- Developing, in collaboration with relevant departments, an IT strategic plan that defines how IT goals will contribute to UMA's strategic objectives and related costs and risks. The IT strategic plan should cover investment and operational budgets, 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.

- Conducting a SWOT analysis for the purpose of reviewing IT strategies, positions, and procedures, and the direction of UMA's IT initiatives. Medium- to long-term goals and directives for future IT-related strategy development are key components of a well-documented IT strategic plan.

Auditee's Response

The campus has been developing a strategic plan over the past few years. Information Technology was engaged in the process from the beginning. Since the strategic plan was focused on the broad needs and directions of the campus, Information Technology was to have been a key part of the second phase of that work given that Information Technologies generally enable business applications, as opposed to deliver functionality independent of business process. The campus will continue to work with the Councils mentioned in the previous response to ensure appropriate coordination and planning of strategic projects and tasks. In addition, in the interim, the Office of Information Technologies will continue its shorter range (1-2 year) planning exercises. Development and/or further refinement of the IT components of the strategic plan will need to be aligned with any changes of direction.

3. IMPROVEMENTS NEEDED IN BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

Our audit indicated that although UMA had 109 department-specific "Continuity Action Plans," UMA did not have formally documented and comprehensive business continuity plans, disaster recovery plans, or continuity of operations plans to provide adequate assurance of the timely restoration of mission-critical and essential business functions should IT systems be rendered inoperable or inaccessible. Additionally, there were no business continuity plans specific to the Lederle Graduate Research Center, which houses the data center where the mission-critical SPIRE application system resides.

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. 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. Sound management practices, as well as industry and government standards, support the need for comprehensive and effective backup 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 to existing business continuity plans. Without a comprehensive and well-documented formal business continuity and disaster recovery strategy for all OIT functions and operations, UMA may be unable to recover mission-critical and essential business activities in an acceptable and timely manner.

Recommendation

UMA should strengthen its disaster recovery and business continuity planning process by:

- Developing and maintaining appropriate recovery strategies to regain mission-critical and essential processing within acceptable time periods. In this regard, OIT should coordinate with business process owners to ensure 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 IT and business process owners to ensure that continuity plans are developed that account for business and IT dependencies.

- Documenting a 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 IT and business operations within required timeframes.

- Developing user area plans to document 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 recovery and continuity planning documents should be available in electronic media, as well as hardcopy format, and be stored off-site in secure accessible locations.

- Annually testing the viability of its alternate processing site, documenting the results of its disaster recovery tests, 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 identify who is to be trained in the implementation and execution of the plans under all emergency conditions.

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

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

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

Auditee's Response

The campus is currently in the process of hiring additional staff within our Emergency Management department to support the ongoing development and refinement of campus Disaster Recovery (DR) and Business Continuity (BC) programs. This new staff member will be charged with the rollout of the SunGard Living Disaster Recovery Planning System (LDRPS) software package that was acquired by the campus to manage this program. This effort will primarily consist of working with campus business units to conduct detail Business Impact Analyses with the business process and technology owners and operators on campus, entering this information in to the LDRPS systems, and developing sustainable workflows to maintain the ongoing operation and maintenance of DR/BC plans. The LDRPS will enable electronic management of resources as well as the ability to create hard copy records as necessary. As part of establishing an effective DR/BC plan, business units will document formal roles and responsibilities documents to ensure clarity and consistency with service restoral during and after incidents that impact campus operations. This program will also include regular testing of the DR/BC plans after completion of the initial documentation. The campus has already begun the deployment of this program and will make steady and regular process. As DR/BC planning is a living and ongoing process, there is not a clear completion date that can be asserted.