UCLA AUDIT & ADVISORY SERVICES

Edwin D. Pierce, CPA, CFE
Director

10920 Wilshire Boulevard, Suite 700
Los Angeles, California 90024-1366
310 • 794-6110
Fax: 310 • 794-8536

September 4, 2015

SENIOR VICE PRESIDENT/CHIEF COMPLIANCE AND AUDIT OFFICER SHERYL VACCA
EXECUTIVE VICE CHANCELLOR & PROVOST SCOTT WAUGH:

Re: Information Technology Services – Enterprise Messaging Audit Report #15-2239

Enclosed is the audit report covering our review of the Information Technology Services Infrastructure Services group. The primary purpose of the audit was to ensure that Infrastructure Services' organizational structure and controls with regard to Enterprise Messaging (EM) were conducive to accomplishing its business objectives. Where applicable, compliance with University policies and procedures was also evaluated.

The scope of the audit included:

- Physical Security and Environmental Controls
- Access Controls
- Communications and Operations Management
- Business Continuity

Based on the results of the work performed within the scope of the audit, Infrastructure Services internal controls are generally conducive to accomplishing the department's business objectives in regards to EM. However, internal controls in the following areas could be strengthened:

- The EM team should ensure that all requests for email creation are compared to the list of authorized submitters.
- Management should review the EM Emergency Response & Recovery Plan and ensure that it is up to date and all necessary personnel are included in the plan.

The corrective actions implemented by management satisfactorily address the audit concerns and recommendations contained in the report. In accordance with our follow-up policy, a review to assess the implementation of our recommendations will be conducted approximately four months from the date of this letter.

Please feel free to contact us if we can be of further assistance.

Edwin D. Pierce, CPA, CFE
Director

Enclosure

cc: S. Olsen

150904-4

INFORMATION TECHNOLOGY SERVICES
ENTERPRISE MESSAGING
AUDIT REPORT #15-2239

Audit & Advisory Services

September 2015

INFORMATION TECHNOLOGY SERVICES
ENTERPRISE MESSAGING
AUDIT REPORT #15-2239

Background

In accordance with the UCLA Administration fiscal year 2014-15 audit plan, Audit & Advisory Services (A&AS) has conducted an audit of the Information Technology Services (IT Services) Infrastructure Services group.

Enterprise Messaging (EM) is a component of the Infrastructure Services group. EM provides email, calendaring, and productivity functions based upon the Microsoft Exchange architecture. These services are delivered to academic and administrative departments. While there are base service level standards, each department has a Service Level Agreement (SLA) to meet their unique operational needs. EM supports over 60 departments and over 120 distinct email domains. There are approximately 22,000 users.

EM is supported with a layered service model that enables departmental Information Technology (IT) staff to work with EM staff to provide end user support. End users are encouraged to contact their department IT as their first point of contact. Department IT staff can call or email the EM Help Desk. Departments can also utilize the Delegated Account Management tools that are made available to appropriately-trained IT staff. All emails to the EM Help Desk are routed to ServiceNow. The ServiceNow tool is an integrated IT Services Management platform that standardizes customer service, making it more efficient.

EM is funded through the Technology Infrastructure Fee (TIF) and is available to interested departments on an opt-in basis. The EM team consists of five system administrators, a Supervisor, and a Systems Operations Manager, who reports to the Senior Director of Infrastructure Services.

Purpose and Scope

The primary purpose of the review was to ensure that Infrastructure Services' organizational structure and controls with regard to EM were conducive to accomplishing its business objectives. Where applicable, compliance with University policies and procedures was also evaluated.

The scope of the engagement focused on the following EM areas:

- Physical Security and Environmental Controls
- Access Controls
- Communications and Operations Management
- Business Continuity

The review was conducted in conformance with the *Internal Standards for the Professional Practice of Internal Auditing* and included tests of records, interviews with key personnel, and other auditing procedures considered necessary to achieve the audit purpose.

Summary Opinion

Based on the results of the work performed within the scope of the audit, Infrastructure Services internal controls are generally conducive to accomplishing the department's business objectives in regards to EM. However, internal controls in the following areas could be strengthened:

- The EM team should ensure that all requests for email creation are compared to the list of authorized submitters.

- Management should review the EM Emergency Response & Recovery Plan and ensure that it is up to date and all necessary personnel are included in the plan.

Audit Results and Recommendations

Physical Security and Environmental Controls

A&AS staff reviewed physical security policies for the Exchange server environment to determine if physical access controls are sufficient. EM personnel were interviewed regarding the environmental and physical access controls relating to the three server rooms. In addition, the three server rooms were physically inspected on June 17, 2015.

Clustered servers are located at three data centers on campus for increased reliability. The data center locations (CSB-1, Jules Stein, and Math Sciences) include uninterruptible power supply (UPS) protection, resilient network connectivity, servers that are on raised racks with seismic bracing and proper grounding, a waterless fire suppression system, automatic backup generators, and a cooling system with a connection to emergency power. They are equipped with temperature and moisture monitors and alarms. Physical access to the server rooms is adequately controlled by an electronic key card system that records individual access to the rooms. The rooms are also equipped with entry alarms and video surveillance.

No significant control weaknesses were noted in this area.

Access Controls

EM system administrators were interviewed regarding access administration. EM policies and procedures for administering user access were also reviewed. The following were noted:

A. User Access

A&AS selected a sample of 15 departments and created a Campus Data Warehouse (CDW) payroll query of employees that were hired by the departments during the period July 1, 2014, to May 31, 2015. A judgmental sample of 15 active EM users from the query was selected to verify that documentation exists to demonstrate that new users were approved by an authorized individual.

- Two of the 15 accounts in the sample were requested by a person that was not on the list of authorized submitters. The request was processed and an account was created.

Recommendation: The EM team should ensure that all requests for email creation are compared to the list of authorized submitters.

Response: Enterprise Messaging will take the action of reminding staff members in writing every six months to compare requestors with those users that are authorized to make changes, and any requests from accounts that are not found to be authorized will be reported to the department for approval.

B. Administrative Access

A review was performed to verify that administrative access to the Exchange database is limited only to necessary personnel based upon job function.

There is no direct access to the Exchange database. EM team members have access to mail databases through their own administrative account. Access to the mail database is appropriately limited to the EM team.

No significant control weaknesses were noted in this area.

Communications and Operations Management

Operational IT controls reviewed included change management, patch management, network security, virus and spam protection, systems monitoring, and backup procedures. The following were noted:

A. Change Management

Change management controls are a formal process used to ensure that changes to a system are introduced in a controlled and coordinated manner. A review of Change Management written procedures, Change Management Meeting Agendas and Minutes, and an example of a Change Management request showed that change management practices are adequate, they include versioning control, documentation, explanation of roles and responsibilities, and adequate separation of duties.

Change Management business practices are enforced through the IT Services Change Management Policy, the Change Advisory Board (CAB), and the Emergency Change Advisory Board (ECAB). The CAB meets regularly; reviews change requests, and approves or disapproves them as appropriate. Membership provides management with adequate understanding of, and control over, changes.

No significant control weaknesses were noted in this area.

B. Patch Management

A&AS staff met with the Senior EM Systems Administrator to discuss patch management. Patch management involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system. There is a standard methodology when applying patches within Infrastructure Services. The method of testing/installing patches is called “standard changes” within ServiceNow. All requests for patches go through ServiceNow and there is a record of each patch that has been applied. Patches are tested in a test environment, which is not a complete mirror of the production environment, but a copy of the functional parts. Patches are monitored and applied within a week.

No significant control weaknesses were noted in this area.

C. Network Security

Network security measures appear adequate. There are access control lists (ACL's) at the router level that control port access to the servers and limits users to logon from certain Internet Protocol (IP) addressees. Source address and destination addresses are controlled.

No significant control weaknesses were noted in this area.

D. Virus Protection

There are multiple layers of malicious software protection available from the EM system. The UCLA SMTP (Simple Mail Transfer Protocol) Gateway uses an anti-virus application to detect virus-infected email. The EM Anti-SPAM (unsolicited email on the internet) appliances include anti-virus functionality to detect viruses. The EM server includes anti-virus software to detect viruses. Microsoft Forefront Protection 2010 for Exchange Server (FPE) is also used which provides protection against malware and SPAM by including multiple scanning engines from industry-leading security partners.

No significant control weaknesses were noted in this area.

E. SPAM Protection

A&AS staff met with the Senior EM Systems Administrator to discuss SPAM protection and filtering techniques. Discussions indicated current SPAM filtering techniques provide adequate protection. Departments have the option of using Proofpoint, Barracuda, or a SPAM software of their choosing. Departments managing their own anti-SPAM solution or SMTP gateway must scan messages using an anti-virus solution before messages are forwarded to EM.

No significant control weaknesses were noted in this area.

F. Systems Monitoring

Server performance is being monitored using the open source network monitoring application Icinga. EM has installed customized scripts to alert EM staff when certain parameters are reached.

Audit/error logs are reviewed as part of the Microsoft Exchange Risk and Health Assessment Program (ExRAP) and ad-hoc reports are generated as a part of troubleshooting procedures.

There are also written procedures for incident handling. A review of the document "Incident Management Process" showed that the procedures met the requirements in the University of California (UC) Business and Finance Bulletin Information Systems (IS Series) - 3, “Electronic Information Security” (IS-3) policy, and include how to document the incident, notification requirements, remediation strategies, and reporting to management.

No significant control weaknesses were noted in this area.

G. Backup

Effective backup and recovery procedures have been established and critical system files and programs are stored at the offsite location Iron Mountain. There are two copies of each database. Full backup is performed once a week and incrementally the other days. The job runs to disk and then to tape the next morning. All tapes go offsite to Iron Mountain.

No significant control weaknesses were noted in this area.

Business Continuity

EM business continuity was evaluated based on discussions with EM personnel and review of the EM Emergency Response & Recovery Plan.

A. Business Continuity Plan

The objective of the plan is to implement a set of defined procedures to respond to and recover from a disruption that involves EM services. Email is a mission-critical application for UCLA, and a preferred method of communication in day-to-day operations. The application is considered a Tier 1 application for a critical group of individuals on the UCLA Campus. The scope of the plan is to provide continuity services until such time that full services can be restored. EM has contracted with Dell MessageOne Email Management Services (EMS) for email storage and access in case of an emergency. Additionally, EM has arranged for redundant servers to be placed off-site at UC Berkeley to provide key back-up services during an outage.

Test work indicated the plan should be reviewed to ensure that it is up to date. There are two people listed in the plan that have separated. One of the employees separated in 2010 and the other in 2012. Discussion with EM management also revealed that there are three people who are not listed in the plan that should be: The Infrastructural Services Director, the IT Services Associate Vice Chancellor, and the IT Services Administrative Director. Without accurate identification of key personnel responsible for emergency procedures, the effectiveness of emergency procedures could be impacted.

Recommendation: Management should review the EM Emergency Response & Recovery Plan and ensure that it is up to date and all necessary personnel are included in the plan.

Response: Enterprise Messaging will take the action of holding annual meetings with Management stakeholders to review/update the EM Emergency Response & Recover Plan, as well as discuss any changes in responsibility. Those changes will then be communicated to the entirety of the Enterprise Messaging team as well as commit updates to the Plan, including any updates in Emergency Response contacts and process updates.

150630-5
REP