INFORMATION TECHNOLOGY SERVICES

ENTERPRISE MESSAGING

AUDIT REPORT #18-2213

Audit & Advisory Services

November 2018

INFORMATION TECHNOLOGY SERVICES

ENTERPRISE MESSAGING

AUDIT REPORT #18-2213

# Background

In accordance with the UCLA Administration fiscal year 2017-18 audit plan, Audit & Advisory Services (A&AS) performed a review of Enterprise Messaging (EM).

Enterprise Messaging provides email, calendaring, and productivity functions based upon the Microsoft Exchange architecture to UCLA academic and administrative departments on an opt-in basis. Enterprise Messaging supports over 65 departments, 27,000 mailboxes, and 200 distinct email domains. Enterprise Messaging is a component of the Information Technology Services (IT Services) Infrastructure Services group and is funded through the Technology Infrastructure Fee (TIF). The EM team consists of five system administrators and a Systems Operations Manager, who reports to the Infrastructure Operations Senior Manager.

Enterprise Messaging currently offers and supports two email system environments, an on-premise Microsoft Exchange and an off-premise cloud-based Microsoft Office 365 (O365) environment hosted and managed by Microsoft. Microsoft Office 365 is offered to campus departments on an opt-in basis. As of October 2017, 14,949 (54%) mailboxes have migrated to O365 and 12,685 (46%) mailboxes remain on the on-premise Exchange environment.

With the O365 cloud-based environments, controls over the following areas are no longer managed by the University, rather they are managed by Microsoft: physical and logical security for the servers and computer equipment, anti-virus and anti-spam, and systems monitoring and availability. Independent third-party examiners regularly audit Microsoft data centers and cloud services, and provide detailed reports that Microsoft makes available for customers to review. While the specific purpose of each audit varies, collectively the audits assess the design and operating effectiveness of O365’s security, compliance, management, and privacy controls. UCLA is still responsible for setting up new user mailboxes and disabling mailboxes for users who no longer require access.

Purpose and Scope

The primary purpose of the review was to ensure that EM’s organizational structure and controls with regard to O365 were conducive to accomplishing its business objectives. The secondary purpose was to evaluate the adequacy and efficiency of internal controls. Where applicable, compliance with University policies and procedures was also evaluated.

The scope of the audit focused on controls surrounding the following activities:

* Migration to Microsoft Office 365
* Microsoft Office 365 Security
* Microsoft Office 365 Agreements
* Availability and Continuity of Microsoft Office 365

The review was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing* and included tests and other procedures considered necessary in achieving the purpose. Interviews were conducted with management and staff, and various other financial and administrative documents were examined.

# Summary Opinion

Based on the results of the work performed within the scope of the audit, controls regarding EM’s O365 systems and processes are generally conducive to accomplishing its business objectives. However, control processes could be further strengthened by implementing the following:

* A list of the authorized submitters and users with access to the Delegated Account Management tool should be provided to each department at least on an annual basis for review and to ensure that all users are active employees and access is still appropriate. Enterprise Messaging should ensure that each Delegated Account Management tool account includes the user’s official name per the UCLA employee database (EDB) and their University Identification (UID) number to enhance the data integrity of the user listing. For the separated employees that were identified during the audit, their Delegated Account Management tool accounts should be disabled or deleted and they should be removed as an authorized submitter. Enterprise Messaging should also remind department IT administrators of their responsibility to provide timely notification to EM when employees separate from the department.
* Enterprise Messaging should ensure that requests from departments to add authorized submitters and assign access to the Delegated Account Management tool are specific as to what is needed and clearly document the request to ensure access to O365 is properly authorized and supported.
* Enterprise Messaging should review the list of accounts with administrator level access on a regular basis to ensure that access is appropriately restricted. In addition, EM should remove the two accounts with global administrator access to O365 that are no longer needed.
* A link to the Allowable Data Use Policy for O365 should be added on EM’s O365 website.
* To minimize the risk of unauthorized access through brute force attacks, EM should consider locking out accounts after a certain number of consecutive invalid attempts.
* Enterprise Messaging should establish a service level agreement (SLA) that is specific to the O365 environment and provide it to campus departments that have migrated to O365.
* Enterprise Messaging should obtain the independent auditors’ reports for O365 from Microsoft and review these reports on an annual basis. One specific report that may be helpful for EM to start with is titled, "Office 365 Architecture and Audit Reports - Management Summary" given that it provides a summary of all the different audits performed. Another audit report that EM should consider reviewing is the System and Organization Controls (SOC) type 2 report, which provides an independent auditor’s opinion on the suitability and operating effectiveness of a service organization’s security, availability, processing integrity, and confidentiality or privacy.

The audit results and corresponding recommendations are detailed in the following sections of this report.

# Audit Results and Recommendations

Migration to Microsoft Office 365

Audit work included discussions with EM management and the Data Center Facilities/Operations & Campus-Wide Projects Director and review of Information Technology Planning Board (ITPB) documents to determine if risk assessments were performed of cloud-based email services and O365 prior to offering the solution and migrating to campus departments. Risk assessments of cloud-based email and collaboration services including risks pertaining to security, data ownership, availability and service levels, and risks of not adopting and leveraging cloud-based services were performed by a UCLA task force comprised of management from IT Services, key campus and Health System departments, and legal counsel.  Specific to security, the conclusion from the risk assessment was that O365 has the ability to satisfy key security requirements for protection of student records, Personal Identifying Information (PII), Protected Health Information (PHI), and sensitive national security or trade data.  Microsoft Office 365 was reviewed and approved by the UCLA Common Systems Group to be offered to all campus departments.

Discussions were also held with the Data Center Facilities/Operations & Campus-Wide Projects Director and Systems Operations Manager to determine if management has evaluated the pros and cons, and the costs and benefits of issuing a directive to require campus departments to migrate to O365. Management indicated that it is more costly to operate and support an on-premise Microsoft Exchange environment versus the cloud-based O365 environment.  Furthermore, with some campus departments still on the on-premise email environment and others on the cloud-based environment, EM needs to support both environments, which adds additional costs. Campus departments are charged the same fee for on-premise and cloud-based email services, thus there is no financial incentive for them to migrate to the cloud even if it is a more cost-effective option. There have been some discussions about issuing a directive to require departments to migrate to O365; however, the Data Center Facilities/Operations & Campus-Wide Projects Director indicated there has not been a mandate, due to other higher priority projects (such as UCPath).

A&AS also had discussions with EM management and reviewed ITPB documents to determine if a pilot project was performed prior to offering O365 to all campus departments.  A pilot project that migrated IT Services to O365 was performed from December 2013 through January 2014. The O365 project was then presented to the UCLA Common Systems Group and approved by them in February 2014 for use by all campus departments. In addition, discussions were held with the EM Supervisor and procedures were reviewed, noting that detailed procedures have been defined to control and manage migrating departments to O365. Furthermore, A&AS had discussions with EM management to verify if training is available to departments and users that migrate to O365, noting that O365 training videos are available on EM's website.  There is an Introduction to O365 video, which helps describe the components of O365, benefits such as increased mailbox sizes and accessibility from any internet connection, and links to other resources and knowledge bases.  Enterprise Messaging’s website includes links to other O365 on-line training classes offered by Microsoft and Lynda.com.

There were no significant control weaknesses found in this area.

Microsoft Office 365 Security

1. Disabling Microsoft Office 365 Accounts

Each campus department has a designated IT administrator or designee responsible for notifying EM immediately when an employee or contractor is no longer employed by the University, so that the account is deactivated to prevent unauthorized use. Authorized department IT administrators or designees can disable the accounts themselves using the Delegated Account Management tool, however, they should also notify EM to remove the account from the system.

Audit work included verifying that authorized submitters and users with access to the Delegated Account Management tool are active employees of the University, separated employees are removed as authorized submitters, and their Delegated Account Management tool accounts are disabled in a timely manner.

A&AS utilized data analytic tools and techniques to compare the names of users with access to the Delegated Account Management tool as of May 30, 2018, to their employment status in EDB. There were 323 user accounts with access to the Delegated Account Management tool; however, 76 user accounts were not recorded because names could not be clearly linked to specific individuals. Without the individuals’ names, a lookup of their employment status could not be performed. Of the remaining 247 user accounts, A&AS compared their names to EDB noting the following:

|  |
| --- |
| **Delegated Account Management Tool Users – Employment Status Check** |
| Employment Status | # of Users |
| Active | 191 |
| Separated | 37 |
| No matching name in EDB | 19 |
| Total | 247 |

|  |
| --- |
| **Authorized Submitter – Employment Status Check** |
| Employment Status | # of Authorized Submitters |
| Active | 263 |
| Separated | 34 |
| No matching name in EDB | 8 |
|   Total | 305 |

Recommendation: A list of the authorized submitters and users with access to the Delegated Account Management tool should be provided to each department at least on an annual basis for review to ensure all users are active employees and access is still appropriate. Enterprise Messaging should ensure that each Delegated Account Management tool account include the user’s official name per EDB and their UID number to enhance the data integrity of the user listing. The UID is a unique identifier and using the employee’s official name adds uniformity. Additionally, by including the UID, data analytics can be performed to ensure that all users are current employees. For the separated employees that were identified during the audit, their Delegated Account Management tool accounts should be disabled or deleted and they should be removed as an authorized submitter. Enterprise Messaging should also remind department IT administrators of their responsibility to provide timely notification to EM when employees separate from their department.

Response: IT Services agrees with the recommendations and will do the following:

1. An authorized users list will be distributed to relevant departments requesting their response and an annual calendar event will be created.

(Due December 15, 2018)

2) Internal procedures will be modified to support official name and UID number in management tool account creation. (Due December 15, 2018)

3) Separated employees identified will have access removed to management tool. (Due November 15, 2018)

4) Separated employees identified will be removed from the authorized submitters list. (Due November 15, 2018)

5) Department IT administrators will be reminded of their notification responsibilities as part of the communication accompanying item #1 above. (Due December 15, 2018)

Note: Our ability to comply with these recommendations is highly dependent upon participation by departments, which has been problematic in the past.

1. Authorized Microsoft Office 365 Users

Each campus department has designated specific individuals that must authorize requests for new O365 user accounts for their employees. Enterprise Messaging maintains a list of these authorized submitters, and checks that requests for new O365 accounts are from a designated individual. A request to add a new authorized submitter must be approved by an existing authorized submitter from the same department.

Authorized departmental IT administrators are granted access to a Delegated Account Management tool, which allows them to perform some O365 user account management functions such as helping to reset the users’ password, disable user accounts, and create and manage email distribution lists.

A&AS reviewed a judgmental sample of ten O365 user accounts that have been defined as authorized submitters and/or also granted access to the Delegated Account Management tool, and verified that their access was approved by an authorized departmental IT administrator or designee. The following were noted:

* Three user accounts, whose requests were submitted by an authorized submitter, did not include specific instructions to setup the user as an authorized submitter nor provide them access to the Delegated Account Management tool.
* Two user accounts that were setup as authorized submitters and granted access to the Delegated Account Management tool, pre-dates the current ServiceNow system where user access requests are submitted and tracked, thus EM management was unable to provide the user access request forms.

Recommendation: Enterprise Messaging should ensure that requests from departments to add authorized submitters and assign access to the Delegated Account Management tool are specific as to what is needed and clearly document the request to ensure that access to O365 is properly authorized and supported.

Response: IT Services agrees with the recommendations and will do the following:

1) Email requests to add authorized users will no longer be allowed.

2) All requests will require a ServiceNow Request.

3) All Request tickets will require EM Manager approval before implementation.

Due: November 1, 2018

Note: A future ServiceNow webform will be suggested/proposed to the Service Management Team.

1. Microsoft Office 365 Administrator Access

Audit work included reviewing user accounts with global administrator access to O365 and user account administrators for Exchange Online to verify that access is restricted to limited, authorized personnel. Administrator access was appropriately restricted to EM and IT Services personnel; however, there was one test account and one migration account, which the EM Technical Lead indicated are no longer needed and should be removed.

Recommendation: Enterprise Messaging should review the list of accounts with administrator level access on a regular basis to ensure that access is appropriately restricted. In addition, EM should remove the two accounts with global administrator access to O365 that are no longer needed.

Response: IT Services agrees with the recommendations and will do the following:

1) A quarterly calendar event will be created to prompt the review and a ServiceNow ticket will be created to record completion.

2) The two accounts identified have already been removed.

Due: November 1, 2018

Note: A future ServiceNow workflow/scheduled event will be suggested/proposed to the Service Management Team.

1. Allowable Data Use Policy for Microsoft Office 365

An Allowable Data Use Policy for O365 has been established that defines the types of data that are permitted and prohibited.  Individual departments are responsible for communicating the policy to their users. Although the policy is available on the UCLA ITPB website, it is not easy to access due to the way the webpage is organized.

Recommendation: An easily identifiable link to the Allowable Data Use Policy for O365 should be added on EM’s O365 website.

Response: IT Services agrees with the recommendations and has done the following:

The EM service pages have all been updated with the Data Use Policy link added:

https://www.it.ucla.edu/services/email-calendaring-collaboration/enterprise-messaging-em

https://www.it.ucla.edu/em

https://www.it.ucla.edu/em-0365

(Data Use Policy link added)

https://godigital.ucla.edu/content/microsoft-office-365-0

Implementation Date: October 12, 2018

1. Microsoft Office 365 Account and Password Controls

Audit work included review of O365 account and password settings, noting that password requirements meet the complexity standards in UCLA Policy 401, Minimum Security Standards for Network Devices. Microsoft Office 365 user account passwords must contain eight characters or more and include at least two of the following three character classes: 1) letters 2) numbers and 3) special characters. Microsoft Office 365 Outlook Web App sessions are set to timeout after six hours, which the EM Technical Lead indicated is appropriate for UCLA users. Microsoft Office 365 user accounts are not currently set to lockout after consecutive invalid login attempts.

Recommendation: To minimize the risk of unauthorized access through brute force attacks, EM should consider locking out accounts after a certain number of consecutive invalid attempts.

Response: IT Services does not agree with the recommendation for the following reason:

1) Denial of Service (DOS) attacks preclude implementing the recommendation.

2) Failed login data reporting/auditing will be enabled instead.

Due: December 1, 2018

1. Security Incidents Notification

Discussions with the EM Supervisor and review of the O365 agreement with the University of California (UC) was performed to determine if the University is notified timely of O365 security incidents. As part of the O365 agreement, in the event of a security incident that impacts UCLA’s O365 cloud-based environment, Microsoft would promptly notify those setup as Global IT Administrators for O365 at UCLA, which includes all the EM team members.  According to the EM Supervisor, there has not been any reportable security incidents related to O365.

There were no significant control weaknesses found in this area.

1. Anti-Virus and Anti-Spam

Audit work included discussions with the EM Supervisor and review of the O365 agreement with the UC, noting that the Exchange On-line Protection anti-virus and anti-spam software is in place for the O365 environment.

There were no significant control weaknesses found in this area.

1. Security Updates and Patches

With O365 being a cloud-based environment, Microsoft is responsible for ensuring that security updates and patches are applied to their systems in a timely manner. A&AS reviewed the independent auditors’ reports to determine that Microsoft updates and patches to their systems are timely, noting that Microsoft’s O365 Security team monitors for known configuration and patching vulnerabilities through automated scans. The criticality of the vulnerabilities are assessed and patches are applied as applicable.

There were no significant control weaknesses found in this area.

1. Physical Security Microsoft Data Centers

Microsoft is responsible for ensuring that physical access to all the systems and devices that support the O365 cloud based environment are adequately secured. Independent auditors perform regular reviews of physical security over Microsoft’s data centers and reports from these reviews are available to O365 customers. Based on the most recent independent auditor's report available at the time of the audit, Microsoft's data centers that host O365 are secured with access restricted to authorized individuals. Below are the controls over the data centers as described in the SOC Type 2 audit report for Microsoft Cloud Infrastructure and Operations, which covered the period of January 1, 2016, through June 30, 2016.

*Physical Security Microsoft Data Centers*: Main access to the data center facilities are typically restricted to a single point of entry that is manned by security personnel. The main interior or reception areas have electronic card access control devices on the perimeter door(s), which restrict access to the interior facilities. Rooms within the Microsoft data centers that contain critical systems (servers, generators, electrical panels, network equipment, etc.) are restricted through various security mechanisms, such as electronic card access control, keyed lock on each individual door, mantraps, and/or biometric devices.

*Access Controls*: The Data Center Management team has implemented operational procedures to restrict physical access to only authorized employees, contractors, and visitors. Temporary or permanent access requests are tracked using a ticketing system. Badges are either issued or activated for personnel requiring access after verification of identification. The Data Center Management team is responsible for reviewing data center access on a regular basis and for conducting a quarterly audit to verify individual access is still required.

There were no significant control weaknesses found in this area.

Microsoft Office 365 Agreements

1. University’s Microsoft Office 365 Agreement with Microsoft

Review of the University’s agreement with Microsoft for O365 indicated there is a formal agreement in place between Microsoft and the University, which includes agreed upon terms and conditions, service levels, and roles and responsibilities.  The agreement was established and signed by the University of California Office of the President and applies to all the UC campuses.  There is not a specific agreement between UCLA and Microsoft.

There were no significant control weaknesses found in this area.

1. Microsoft Office 365 Service Level Agreements (SLA) with Campus Departments

A&AS had discussions with EM management to verify if agreements are in place between EM and campus departments defining the service levels, and roles and responsibilities specific to O365.

There is a standard SLA between EM and campus departments that still utilize the on-premise Microsoft email system; however, there is not a SLA specific to departments that have migrated to a cloud-based O365 environment.  The on-premise SLA includes terms and conditions that are not applicable or different for the O365 environment such as the following:

* User support and trouble reporting timeframes
* Incident response
* Message data backup, archival and restoration
* Mailbox size limits
* SPAM management system
* Anti-Virus system
* Uptime standards
* Disaster Response Email Continuity Program
* Equipment maintenance and upgrades

In addition, the SLA includes outdated terminology such as Blackberry and PDA (Personal Digital Assistant) devices.

Recommendation: Enterprise Messaging should establish a SLA that is specific to the O365 environment and provide it to departments that have migrated to O365.

Response: IT Services agrees with the recommendations and will do the following:

1) An Office 365 specific SLA will be created. (Due January 15, 2019)

2) The new SLA will be distributed for signature/review. (Due June 30, 2019)

Note: Completion of item #2 above is highly dependent upon participation from departments, which has been problematic in the past.

Availability and Continuity of Microsoft Office 365

Audit work included discussions with management, review of the agreement the University has with Microsoft and the independent auditor’s report to determine if Microsoft's cloud-based environment for O365 includes redundant systems and replication of data to ensure the availability of O365 applications and supporting services.  In addition, A&AS reviewed the SLA for Microsoft On-line Services to determine if email service availability guarantees are included.

Microsoft's cloud-based environment for O365 includes highly redundant systems and robust replication of data to ensure the availability of email to the University. Microsoft Office 365 data is replicated in real-time to multiple servers and locations including to another server in same data center and also to two geographically dispersed data centers. Failover exercises are conducted on a regular basis to verify the accessibility of systems and data at a secondary disaster recovery location. According to the independent service auditor’s report for O365, the redundancy and replication processes stated above are in place to ensure the availability of email systems in the event of a disaster.

Microsoft provides a SLA for O365, which guarantees 99.9% uptime.  Overall uptime for O365 exceeded the 99.9% for 2016 through the first quarter of 2018 based on statistics published on Microsoft’s website.

There were no significant control weaknesses found in this area.

Independent Auditors' Reports – Controls at Microsoft's Office 365 Cloud Environment

With O365 being a cloud-based solution that is hosted by Microsoft, the responsibility for security, availability, and integrity of the email system is shifted from the University to Microsoft. Third party examiners perform regular audits of Microsoft’s O365 cloud environment and provides their independent opinion on the suitability and operating effectiveness of controls at Microsoft to ensure the security, availability, processing integrity, and confidentiality of the O365 environment. Reports from the audits are available to the University for review; however, these reports have not been requested and reviewed. Since O365 customers span many different industries, each with their own compliance requirements and best practices, there are many different audit reports, which address compliance with different standards, components of the O365 environment, and timeframes.

Recommendation: Enterprise Messaging should obtain the independent auditors’ reports for O365 from Microsoft and review these reports on an annual basis. One specific report that may be helpful for EM to start with is titled, “Office 365 Architecture and Audit Reports - Management Summary" given that it provides a summary of all the different audits performed. Another audit report that EM should consider reviewing is the SOC type 2 reports, which provides an independent auditor’s opinion on the suitability and operating effectiveness of a service organization’s security, availability, processing integrity, and confidentiality or privacy.

Response: IT Services agrees with the recommendations and will do the following:

1) An annual calendar event will be created to prompt the review and a ServiceNow ticket will be created to record completion.

2) This year’s review has already been completed.

Due: November 1, 2018

180627-2

REP