Assurance Report

1930 Microsoft Office 365 Implementation

June 24, 2020

Cindy Rougeou, LASERS Executive Director
The LASERS Audit Committee

BACKGROUND

This was a planned engagement on the fiscal year end (FYE) 2020 Audit Plan. The fieldwork for this engagement was completed on June 4, 2020.

LASERS IT (IT) division solicited a request for proposal to migrate the on-premise email system to Microsoft Office 365, a secure cloud based email solution. The main project focus was to transition the Microsoft Exchange (Exchange) Server to a secure cloud server from Microsoft, allowing the email system to remain functional with no interruption or delay in the event of a disaster.

The Microsoft Office 365 transition was completed by IT staff with the assistance from other divisions during the pilot. LASERS utilized contract services from Sparkhound, a Microsoft Gold Partner, to assist with the implementation. Along with Sparkhound, one of their subsidiaries, Archive360, assisted with the migration of LASERS email archives stored in EMC SourceOne to the Microsoft Exchange Server on-premise.

SCOPE, OBJECTIVES, AND METHODOLOGY

The scope of this engagement covered the planning and implementation phases of the Microsoft Office 365 project.

The primary objectives of this engagement were to determine if:
- The Microsoft Office 365 email and related products have adequate controls in place to protect

LASERS data.
- Microsoft meets all LASERS security requirements and has obtained certain third party security certifications.
- The implementation and configuration of Microsoft Office 365 email and related products within the LASERS environment align with leading practices.
- LASERS email archive is properly migrated to each mailbox.
- LASERS data is properly migrated to Microsoft Azure.
- LASERS has implemented a cloud based back-up solution for the email system.
- LASERS email system is expected to remain functional in the event of a disaster.

Procedures used to complete this engagement included:
- Consulting with IT to ensure the project met all objectives.
- Reviewing the security documentation to confirm if Microsoft met LASERS security standards.
- Assisting with the review of the documentation submitted to executive management and other key stakeholders requesting approval to perform a pilot test of Microsoft 365 with select LASERS staff.
- Confirming the vendor successfully migrated LASERS email archive to Microsoft Exchange.
- Confirming the vendor successfully migrated all LASERS mailboxes to Microsoft Office 365.
- Ensuring an email backup solution is in place.
- Reviewing documented procedures for account creation in Microsoft Office 365.
- Determining if the implemented solution allowed for email to remain available and function in the event of a disaster.
- Conducting other inquiries considered necessary to achieve engagement objectives.

This engagement was conducted in accordance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing and the policies and procedures of the Audit Services Division.

ENGAGEMENT SUMMARY

_____
1.   SECURITY REVIEW AND MICROSOFT OFFICE 365 PILOT APPROVAL

SUMMARY
Before requesting approval to pilot Microsoft 365, IT obtained a Cloud Assessment conducted by Phidiax and a Microsoft Office 365 Discovery Readiness Assessment and Design conducted by Bishop. One item received from these assessments were some outlined pros and cons of switching to a cloud based email system. Some of the key pros to this system included a reduction of a resource footprint in the data center, decrease in costs and administrative needs, elimination of email archive services, and easier management of a single platform to deliver email, collaboration, and messaging services. The following cons were outlined (response from IT included):
1. Risk of potential vendor service outages: IT understands there could be potential vendor outages, but Microsoft has detailed service outage maps and works diligently to restore services quickly.

2. Migration may be time consuming and may require professional services costs for migration: IT understands that a vendor will be required to complete the migration and a scope will be defined to ensure data is properly transferred.
3. Dependency upon internet connectivity: IT has added a redundant internet line through a separate vendor. In the event of an internet outage, LASERS will manually switch connection to a second vendor. IT is working with the vendor to form an agreement and configure the internet connection to automatically failover to the second connection in the event of an outage.

At the conclusion of these assessments, IT determined that Microsoft Office 365 would be a good transition for LASERS and began reviewing the security components. Microsoft Cloud Services are built on a common distributed fabric with physical and logical separation such as regions, government versus commercial, and national clouds. The security documentation was provided for Microsoft Azure, Microsoft's cloud computing platform, since they also apply to services such as Microsoft Dynamics 365 and Office 365. One of LASERS established security standards require that each new cloud vendor obtain a Cloud Security Alliance Security Trust Assurance and Risk (CSA STAR) Certification, ISO 27001 Certificate, and a Systems and Organization Controls (SOC) 2, Type 2 audit before being utilized at LASERS. IT and Audit Services staff reviewed the security documentation provided and confirmed that Microsoft exceeded LASERS current security standards. Along with the LASERS defined security requirements, Microsoft has also obtained the Federal Risk and Authorization Management Program (FedRAMP) certification designed by the Federal Government so agencies do not have to analyze the cloud computing services, but can rely on this certification for meeting the highest level of compliance.

After the confirmation that Microsoft met LASERS security standards, IT created the Microsoft Office 365 Pilot Approval document which was analyzed and reviewed by Audit Services before it was shared with all parties (i.e., members of the executive team, division directors, legal counsel, and chief risk officer) requesting approval.

Upon receiving unanimous approval, the Microsoft Office 365 pilot was conducted in two phases:
- Phase one consisted of IT staff performing further testing and evaluation of the Microsoft Office 365 service. After a test period with no adverse effects, IT recommended a transition to phase two.
- Phase two consisted of LASERS Investment staff testing the email service and other services used for Contact Management, such as Microsoft Dynamics 365. After a test period with no adverse effects, IT recommended the implementation of Microsoft Office 365 to the remainder of the LASERS staff in a phased approach by division. IT chose Sparkhound as the lead vendor for the implementation.

There are no outstanding items related to the security and pilot of Microsoft Office 365.

_____

2.   EMAIL ARCHIVE MIGRATION

SUMMARY
LASERS previously utilized an email archiving tool called ECM SourceOne (SourceOne) which stored all emails from each employee's mailbox. This system required the user to access a separate database to view all archived emails sent or received. Before migrating the email accounts to Microsoft Office 365, IT determined that the archived emails had to first be migrated to the on-premise Microsoft

Exchange Server. With the assistance of a vendor, Archive360, archived emails were migrated from SourceOne. A full backup of SourceOne was made at the conclusion of the migration before SourceOne was decommissioned. Therefore, information can be retrieved from this backup in the future, if needed.

According to Archive360, the complex structure of SourceOne did not allow IT or Archive360 to pull a report directly from the system showing the number of emails, per mailbox that was expected to be migrated by Archive 360 to Microsoft Exchange. According to Archive360, SourceOne is used differently by each organization who purchases the system and there are no stored reporting utilities. This required Archive360 to develop their own utility software that extracted data from SourceOne which then allowed reports to be generated by them.

In addition to the vendor's validation, independent testing was performed by Audit Services to reasonably confirm success of the archive migration. It should be noted that Audit Services did not confirm email content including email size as part of this testing. The details and conclusions from this independent testing is as follows:

a. Audit Services obtained a listing of all active LASERS email accounts from LASERS IT and compared it to a list of accounts that Archive360 migrated to Microsoft Exchange. All applicable LASERS accounts with data in SourceOne were successfully migrated. Inactive accounts were not migrated since this would have required each inactive mailbox to be rebuilt in Exchange. However, information can be retrieved from the SourceOne backup for the inactive accounts, if needed.

b. Archive360 provided an initial migration report to IT showing a list of all email accounts that were migrated from SourceOne to Exchange along with the associated item count. Audit reviewed this report and performed sample testing to confirm message counts between the Archive360 report and counts from Microsoft Exchange. Instances were identified where emails found in SourceOne could not be found in Exchange. After consulting with IT and Archive 360, it was determined that SourceOne stored emails as two different types, Exchange (EX) or Simple Mail Transfer Protocol (SMTP), and only the EX type emails were initially migrated.

After discussions with IT and Archive360, it was determined that the count of the EX type emails that were initially migrated to Exchange could not be explicitly confirmed against SourceOne. The primary reason for this was that the initial migration of the EX type emails from the SourceOne archive were migrated into the LASERS live Exchange on-premise environment where active mailbox archiving was occurring at the same time as the migration. This resulted in a difference in the item counts per Archive 360 reports and Exchange. Due to the migration already being started and the difficulty with undoing this process and restarting, it was decided by IT to not roll back that initial migration. Given these circumstances, Audit Services requested that a sample of two email accounts have their EX type emails re-migrated into a separate archive folder within their mailbox in Exchange for validation. Audit Services was able to explicitly confirm that the migrated EX type email item counts between SourceOne and Exchange matched for these two accounts. This limited testing helped provide some assurance on the migration process developed and performed by Archive360 by confirming the counts for the Exchange mailbox matched the Archive 360 report in these two instances. Since Audit Services could not explicitly confirm the email counts of all EX type emails, reliance was placed on the assurance provided by Archive360 confirming that all EX type emails were

migrated.

Once the EX type emails were successfully migrated, it was decided that Archive360 would migrate the SMTP type emails to a separate archive inbox folder on Exchange entitled, "SMTP". In addition, Sparkhound and their team would provide a report showing the number of email messages in the SMTP folder in Exchange. This approach would allow for the ability to effectively compare item counts between Archive360's report and Exchange. After receiving the reports from Archive360 and Sparkhound, Audit Services performed a comparison between the item counts from the Archive360 report to the Sparkhound report. With the exception of one user, all counts matched. One user was missing 35 email messages, but it was determined to be immaterial since Archive360 was unable to identify which emails did not successfully migrate. The user with the possible missing email messages confirmed that there were no identifiable differences in their archive mailbox on Exchange. Furthermore, Audit Services performed additional testing to reasonably confirm the reliability of the reports provided by Archive360 and Sparkhound by selecting a sample of 16 LASERS staff and requesting the item count in their SMTP folder. No exceptions were identified from this testing.

At the end of the migration, Archive360 provided a final report detailing all migration jobs completed and their status along with all exceptions noted throughout the project. The report stated that all necessary inboxes were properly migrated to the Exchange archive. The archive migrations took place between May 21, 2019 and October 17, 2019 and since the final migration, IT has not received any notification from a user that archived emails are missing. In the event that an email is reported missing, IT is able to restore all archives from the backup completed post migration. All exceptions noted in the Archive360 final report are considered closed.

The email archive migration to Microsoft Exchange has been deemed successful and there are no outstanding items.

_____
3.   EMAIL MICROSOFT OFFICE 365 MIGRATION

SUMMARY
After completion of the archive migration to the on-premise Exchange, LASERS consulted with Sparkhound to complete the migration to Microsoft Office 365. As part of their migration process completed after the initial pilot testing, Sparkhound generated reports showing the mailbox item counts before and after the migration. Separate reports were also required for the archive data showing the item counts before and after the migration. A full backup of the on-premise Exchange was made at the conclusion of the migration before Exchange was decommissioned. Therefore, information can be retrieved from this backup in the future, if needed.

In addition to the vendor's validation, independent testing was performed by Audit Services to reasonably confirm success of the migration to Microsoft Office 365. It should be noted that Audit Services did not confirm email content including email size as part of this testing. The details and conclusions from this independent testing is as follows:

a.   Audit Services obtained a listing of all active LASERS email accounts from IT and a listing of all active LASERS employees and compared each to a list of accounts that Sparkhound

migrated to Microsoft Office 365. During this testing, Audit Services identified 49 active mailbox accounts that had not been migrated to Microsoft Office 365. Of the 49 accounts, only one was for an active LASERS employee. These 49 mailbox accounts were later migrated and conversion reports were provided confirming this. All active mailboxes were successfully migrated and inactive accounts were included on the back up and can be restored, if needed.

b. Audit Services performed an analysis of the before and after reports to confirm the items counts and evaluate any differences. The details of this analysis is as follows:
   i. Regarding the archive data, there were issues with the reports generated by Sparkhound. According to Sparkhound, they did not use the correct parameter when pulling the archive data which caused the inclusion of folders used only by Microsoft administrators. The mailbox item counts of these folders were included in the report for Microsoft Office 365 and not for Exchange which created the differences. Since Audit Services could not explicitly confirm the item counts for the archive, reliance was placed on the assurance provided by Sparkound confirming that all archive data was successfully migrated to Microsoft Office 365. IT has not received any notification of missing archive emails in Microsoft Office 365 from any staff members since the migration completed in October 2019.
   ii. Regarding the non-archive data, the migration and analysis consisted of a comparison between the item counts from the inbox, sent items, and deleted items. In general, the analysis was separated and completed by division and the details are as follows:
      - **Fiscal Staff Migration:** Sparkhound pulled reports before and after migration to use for mailbox comparison. These reports utilized for comparison were pulled two and a half days apart and since individuals were actively utilizing their email accounts, materiality tolerances were set. All mailbox accounts with positive differences higher than 150 and negative difference higher than 30 were analyzed. The calculated differences for one individual exceeded the tolerances for the sent items and Audit Services confirmed that the individual had sent that exact number of emails that matched the difference. No calculated differences exceeded the tolerances for the inbox and deleted items.
      - **Audit Services, Executive, Human Resources, Legal, Member Services, and Public Information Migration:** Sparkhound pulled reports before and after migration to use for mailbox comparison. These reports utilized for comparison were pulled one day apart and since individuals were actively utilizing their email accounts, materiality tolerances were set. All mailbox accounts with positive differences higher than 50 and negative difference higher than 30 were analyzed. No calculated differences exceeded the tolerances for the inbox, sent items, and deleted items.
      - **Service Account Migrations:** Sparkhound pulled reports before and after migration to use for mailbox comparison. These reports utilized for comparison were pulled one day apart and since these accounts were actively being utilized, materiality tolerances were set. All mailbox accounts with positive differences higher than 50 and negative difference higher than 30 were analyzed. No calculated differences exceeded the tolerances for the inbox, sent items, and deleted items. There were some issues encountered with two accounts, Rightfax and Tidal, which required additional steps. Once these accounts were updated, Sparkhound provided conversion reports showing these accounts were successfully migrated.

- **Investments and IT Migration:** Investments and IT staff mailbox accounts were migrated in September and October 2019 as part of the pilot testing. Reports showing the item counts in Exchange before the migration took place were not generated. To document the migration's success, IT requested from Sparkhound copies of the logs showing that the mailboxes were migrated. Unfortunately, these logs were not saved by Sparkhound and were automatically deleted after 60 days. Sparkhound was able to pull reports for two IT staff members showing their accounts were successfully migrated. Since no comparison reports were generated to confirm that all mailbox items were migrated successfully, audit cannot explicitly confirm this. However, there does not appear to be any issues with the migration of these mailbox accounts since IT has not received any notification from a user that emails are missing in Microsoft Office 365.

At the end of the migration, Sparkhound provided a final report detailing the status of the project. The report stated that Sparkhound successfully migrated the LASERs on-premise mailboxes to Microsoft Office 365 and all exceptions are closed. Since the migration to Microsoft Office 365, IT has not received notification that any emails are missing. In the event that an email is reported missing, IT is able to restore all Exchange mailboxes from the backup completed post migration.

The migration to Microsoft Office 365 has been deemed successful and there are no outstanding items.

_____

4. NEW EMAIL ACCOUNT CREATION IN MICROSOFT OFFICE 365

SUMMARY
Audit Services confirmed that IT properly documented the steps to create a new email account in Microsoft Office 365. Detailed procedures were created to document this process along with the steps to create the corresponding email account archive. Audit Services reviewed these procedures and confirmed the process was properly documented. There are no outstanding items related to the new email account creation in Office 365.

_____

5. EMAIL DISASTER RECOVERY

SUMMARY
After the implementation of Microsoft Office 365, IT addressed two disaster recovery items related to the email system. IT implemented a new cloud based backup solution of the email system and determined updates needed to ensure LASERS email was functional in the event of a disaster where the LASERS on-premise data center is unavailable. The details for each of these items are as follows:

a. IT began backing up LASERS email system to a cloud based solution, iLand. This will allow LASERS to restore the email system to a previous point in time, in the event this would be needed. LASERS previously saved backup files for the email system to tape; therefore, the cloud based solution replaced this going forward. The implementation of this new approach did not change the backup rotation schedule.

b. It was determined that in the event of a disaster where the LASERS on-premise data center is unavailable, employee email functionality would not be automatically available. The primary

reasons for this is that emails to and from LASERS email addresses flow through IronPort, LASERS spam filtering solution, and fax to email capabilities, which is stored on a server at LASERS. After discussions with IT, it was determined that emails needed to be re-routed directly to the Microsoft cloud instead of passing through servers at LASERS. IT management approved the implementation of Mimecast, a cloud email security platform. This implementation was tracked in a separate project and Audit Services participated in a consulting capacity. This implementation has been completed and LASERS email will be fully functional in the event of a disaster where the data center is unavailable.

There are no outstanding items related to the email disaster recovery components.

FOLLOW-UP

No follow-up is necessary.

Reece Babin
Auditor

Ryan Babin, CIA, CISA
Audit Services Director

Cc: Trey Boudreaux
        Dan Bowden
        Eric Schoonmaker
        Greg Byrd