Maricopa County Library District
Audit of Information Technology
By Maricopa County Internal Audit
December 2020

Why This Audit Is Important

The Maricopa County Library District (MCLD) operates 18 libraries in Maricopa County offering access to a wide variety of on-site and electronic services to surrounding communities. Services include providing books and other hard-copy materials, special programs and events, and electronic resources such as eBooks, audiobooks, movies, music, computers, and Wi-Fi access. MCLD relies heavily on its information technology resources to support the services they provide county residents.

We performed this audit to assess whether MCLD has established adequate controls for (1) granting and monitoring access to key data center applications, (2) restoring operations in the event of a disaster or unplanned interruption, and (3) data center operations and security.

Key Findings

- Management of user access can be strengthened through written procedures and periodic reviews of access rights.
- Adequate data backup processes were in place, but related written procedures are needed.
- Continuity of operations and disaster recovery plans should be enhanced and completed, including written procedures for testing and review.
- Data center operations addressed essential monitoring and security practices; however, some key controls can be improved through periodic checks and written procedures.

All key findings requiring corrective action were addressed through agreed-upon management action plans.

What We Audited

Following is a summary of work performed and findings. Corresponding recommendations and responses start on page 3. The responses were approved by Jeremy Reeder, MCLD Director, on October 20, 2020. More detailed observations and recommendations were communicated to management throughout the audit process.

Application User Access

Background – User access controls over software applications can help ensure that access to data is limited based on job duties, promptly removed upon termination, and regularly reviewed to ensure all users are appropriately granted application access. We interviewed key employees, reviewed documentation, and performed sample testing to assess controls over managing access requests and changes to eight key data center management applications and MCLD's badge access software applications.

Observations – Application user access was appropriately restricted based on job duties. However, formal approval for granting access was not documented and there were no written policies and procedures for access management (**Recommendation 1**). In addition, periodic user access reviews were not performed to help ensure that user access is monitored for appropriateness, based on current job responsibilities (**Recommendation 2**).

Contingency Planning and Backup

Background – Contingency planning efforts help ensure critical operations can be restored in the event of a disaster or unplanned interruption. Contingency planning often includes (1) a disaster recovery plan that addresses restoring technology infrastructure and systems, and (2) a continuity of operations plan that establishes policy and guidance to ensure critical business functions continue in the event of an emergency. We interviewed key employees and reviewed continency planning and backup documentation to assess controls for restoring operations in the event of a disaster or unplanned interruption.

Observations – Nightly and weekly data backups were performed, and backups were replicated to an off-site facility. The MCLD's continuity of operations plan lacked necessary IT components, and there was no disaster recovery plan in place (**Recommendation 3**). Detailed observations and gaps were communicated to management. MCLD has not established policies or procedures for contingency planning or data backup and recovery (**Recommendation 4**).

Data Center Monitoring

Background – Effective data center monitoring of operations, equipment utilization, processing, and security threats can prevent the waste of resources and unfavorable performance or availability issues. We interviewed key employees and reviewed documentation for MCLD's monitoring controls over data center operations and security management processes.

Observations – MCLD oversees data center equipment operations and utilization through manual monitoring and reporting while adhering to informal procedures for patching and updating servers and operating systems. System security management software is used to help prevent and deter possible security threats. MCLD monitors and reviews security management logs and notifications but does not consistently retain documentation. There are no written policies and procedures for data center operations/utilization or for governing security management processes (**Recommendation 5**).

Physical Security

Background – Data centers provide a protected location for the equipment that stores, manages, and disseminates data used to support critical business operations. To protect these assets, the facility must have proper power, cooling, and fire suppression. Physical access to the facility should be limited and regularly reviewed to ensure only those with a business need have access.

Observations – We interviewed employees, reviewed documentation, toured one MCLD data center, and reviewed lists of those with badge access to MCLD's data centers for two MCLD data centers. We observed the following:

- Data center controls used to protect sensitive technology resources in the event of environmental hazards (water, fire, humidity, temperature, etc.) were adequate.
- Physical access to one data center was appropriately restricted; however, physical access to the other included terminated individuals or individuals with inappropriate access. Periodic reviews of access lists were not performed (**Recommendation 6**).
- There were no written physical access policies and procedures for controlling physical access to its data centers (**Recommendation 7**).

Additional Information

This audit was approved by the Maricopa County Board of Supervisors and was conducted in conformance with International Standards for the Professional Practice of Internal Auditing. This report is intended primarily for the County and its stakeholders. However, this report is a public record and its distribution is not limited. If you have any questions about this report, please contact Mike McGee, County Auditor, at 602-506-1585.

Recommendations and Responses

Recommendations	Responses
1 Periodically review a current list of user accounts to the key data center software applications, and the badge access management software, to ensure granted access is appropriate based on job duties.	Concur – in progress Will schedule periodic reviews. Target Date: 1/20/2021
2 Establish written policies and procedures addressing granting, modifying, removing, and regularly reviewing user access to key MCLD applications.	Concur – in progress Will create policies and procedures. Target Date: 7/25/2021
3 Complete the MCLD COOP and/or establish a disaster recovery plan to ensure critical data and equipment are adequately protected from loss or destruction in the case of a disaster or other unplanned event.	Concur – in progress Will complete COOP and establish disaster recovery plan. Target Date: 7/25/2021

Recommendations	Responses
4 Establish written policies and procedures to ensure the following: • The COOP and/or the disaster recovery plan is regularly reviewed, updated, tested, and communicated to MCLD employees. • Data backup and storage processes adequately protect critical data from loss or destruction.	Concur – in progress Will establish policies and procedures. Target Date: 7/25/2021
5 Establish written policies and procedures to ensure the following: • Data center operations include efficient equipment operations, utilization, and processing. • Adequate security threat identification, monitoring, response, and reviews.	Concur – in progress Will establish policies and procedures. Target Date: 7/25/2021
6 Periodically review current badge access to MCLD managed data centers and remove all individuals listed that do not require access for performing their job duties.	Concur – in progress Will schedule periodic reviews. Target Date: 7/25/2021
7 Establish written policies and procedures addressing granting, modifying, removing, and regularly reviewing physical access to MCLD's data centers.	Concur – in progress Create policies and procedures. Target Date: 7/25/2021