RSM US LLP

19026 Ridgewood Pkwy
Suite 400
San Antonio, TX 78259

T +1 210 828 6281

www.rsmus.com

March 27, 2018

To Management
Edwards Aquifer Authority
San Antonio, Texas

In planning and performing our audit of the financial statements of Edwards Aquifer Authority (the EAA) as of and for the year ended December 31, 2017, in accordance with auditing standards generally accepted in the United States of America, we considered the EAA's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the EAA's internal control. Accordingly, we do not express an opinion on the effectiveness of the EAA's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis. A deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective would not be met. A deficiency in operation exists when a properly designed control does not operate as designed or when the person performing the control does not possess the necessary authority or competence to perform the control effectively.

A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis.

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

The following are descriptions of identified deficiencies in internal control that we determined did not constitute significant deficiencies or material weaknesses.

Ability to Post and Approve Journal Entries

Observation: We noted the Controller, Executive Director of Administration and Finance and the Deputy General Manager all have access to both post and approve journal entries. These individuals all have supervisory roles and responsibilities and, thus, their ability to post journal entries should be eliminated if possible.

Recommendation: Even though there is currently no activity of these individuals performing these functions, since the original intent was for them to serve as backup personnel, under a sound system of internal controls, these are incompatible functions. We recommend management consider evaluating if other personnel not in a supervisory role should be setup as the backup instead.

Management response: The finance department is undergoing changes in management structure with the addition of a new position in 2018. This will allow the requisite controls, as identified, to be implemented this year (2018).

Consider Adequacy of the Controller Being the Primary Administrator of the Accounting Application

Observation: As part of access review procedures performed, we noted the Controller is the primary administrator of the accounting application.

Recommendation: We recommend management consider designating someone else to take over this role and/or develop specific control procedures which mitigate the risk of incompatible functions that could exist with the Controller being the primary administrator.

Management response: As mentioned, the introduction of a new layer of management and oversight with a new position in the finance department in 2018 will provide the opportunity to review and refine controls of the accounting system. The EAA will review best management practices of other governmental entities to introduce measures in keeping with audit recommendations.

General Information Technology Control Environment

As part of our review of the EAA's internal control environment, we also performed a review of the overall design of the information technology controls that could potentially have a direct or indirect impact on financial reporting. Based on our understanding of the overall design, we have identified certain areas which, in the aggregate, represent a control deficiency over the general information technology control environment of the EAA.

- ***Monitoring of user accounts related to accounting application***

  Observation: As part of our review of the accounting application user report, we identified seven user accounts that belong to a vendor who has administrative access to the application. This access allows them to not only modify configuration, but also to potentially post entries to the system. Management indicated the access was granted as part of the initial system implementation; however, subsequent to completion of the implementation, this access should have been limited or deactivated and only used as needed to resolve issues based on service tickets submitted to the vendor.

  Recommendation: We recommend management assess the need to maintain vendor user accounts and, if such need is there, to consider establishing a process to only activate vendor user accounts as needed. The process should also call for active monitoring of vendor activity.

  Management response: In 2017, it was necessary to involve the assistance of the accounting software consultants as the software was deployed, assist in on going training or deploy new facets of the software after initial implementation. Staff will ensure a termination date for access is entered upon granting access in the software and monitor third-party vendor monthly access log reports.

- ***Monitoring of users with access to the network***

  Observation: We noted no review is currently performed over users who have access to the network.

  Recommendation: We recommend management perform a review of network accounts on a periodic basis to ensure access is limited to only active employees.

Management response: The EAA is upgrading network infrastructure and servers, which will allow for appropriate controls to be implemented in late 2018 or early 2019. New controls will allow for the auditing of user access reports on a monthly basis, which will be consistent with this recommendation.

- ***Monitoring of vendor service organization controls (SOC) reports do not exist***

  Observation: SOC reports are required to be provided by organizations that are either processing or hosting the EAA data. The report ensures vendors have adequate processes and controls in place to secure the EAA data. We noted no reviews are currently being performed over SOC reports for critical vendors, defined as vendors who either host or process information for the EAA.

  Recommendation: We recommend management perform a review of the SOC reports, along with user entity controls. Management should also document compliance with user entity controls, as documented within the respective SOC reports. In addition, as part of its annual due diligence, management should also review the respective vendor's financial statements when available.

  Management response: In 2018, the EAA will develop a formalized procedure to review SOC reports for critical vendors who host or process EAA information. The procedure will include documentation of each SOC reviewed, as well as the compliance with user entity controls.

- ***Limit server room access to appropriate personnel***

  Observation: Per discussion with information technology personnel and review of the badge access report, it was determined all EAA employees with a badge have access to the server room.

  Recommendation: We recommend management limit access to the server room in accordance with each employee's job description.

  Management response: In February 2018, purchases were made to update the software and hardware that control door access points at the EAA, including access to the server room. Once the software and hardware are configured, access to the information technology server rooms will be restricted to information technology personnel.

- ***Formal process is not in place to add/remove employee access from the accounting system***

  Observation: We noted a formal process is not in place to add or remove employee access from the accounting system. As part of the user access review, we identified one instance where employee access was removed almost 20 days subsequent to employee termination.

  Recommendation: We recommend management establish a formal process to ensure access granted to employees is adequately approved and in accordance with their respective job descriptions. For terminated personnel, we recommend management establish a policy to ensure timely removal of all employees from the network along with the accounting application.

  Management response: Staff is formalizing a procedure for accounting software access assignments/ roles to be approved and assigned to employees based on job description, as well as the addition and removal of users from the accounting software. This process will be incorporated with the EAA new hire procedures and out-processing of exiting employees. Currently, a manual process does exist for notification to add/remove employee access from accounting system. This new procedure will be automated through a new or terminating employee service ticket system.

- ***Lack of enterprise-wide business continuity plan and disaster recovery plan***

  Observation: We noted the EAA does not have an enterprise-wide business continuity plan or a disaster recovery plan.

  Recommendation: We recommend management consider such plans be developed to prevent interruption of normal operations and to allow for the resumption of business processes in a timely manner. In addition, we recommend management consider conducting tabletop exercises within various departments to ensure employees are familiar with their individual responsibilities in a disaster situation.

  Management response: In 2018, the EAA is upgrading its network infrastructure to allow for adequate backup and recovery of critical data in the event of a disaster. These upgrades will conclude in 2018 and the EAA will then develop, document and test the disaster recovery plan to include roles for key users of the system.

- ***Evaluate the overall environmental controls of the server room***

  Observation: Based on observation procedures performed, we noted the server room has an active water sprinkler in place. In addition, there is no temperature alert mechanism currently installed.

  Recommendation: We recommend management evaluate the overall environmental controls and make enhancements as needed to limit the overall loss in a disaster situation.

  Management response: In 2018, staff is committed to capping the server-room sprinkler, installing a temperature sensor and placing a fire extinguisher in the server room to limit the risk of water or fire damage to the EAA's servers and data.

- ***Offsite backup for the domain controller***

  Observation: We noted no offsite backup is currently being maintained for the domain controller.

  Recommendation: We recommend management consider having an offsite backup of the domain controller to ensure network configuration, user profiles and shared files are accessible in a disaster situation.

  Management response: Additional space at an adjacent EAA building has been secured to house a back-up of the domain controller. In addition, the domain controller has been added to the list of cloud-based (AWS) backups currently being captured by an EAA third-party vendor. In 2018, the EAA is looking to implement a three-part backup system at different off-site locations.

- ***Permitting application no longer supported by vendor***

  Observation: We noted the permitting application used by the EAA is currently hosted on a Windows 2003 server that is no longer supported by the vendor. As a result, no security updates are being applied to the server, which increases the risk of overall vulnerabilities and potential network compromise.

  Recommendation: We recommend management establish a plan to upgrade the servers that are no longer supported by the vendor. In addition, management should also consider implementing processes to monitor user activity at both the application and server level.

Management response: This situation will be remedied when the new EAGIS database development is completed in 2019, as this new system is being constructed on a Windows 2010 Azure server.

In 2018, the EAA will also install an internal firewall that will track usage of all internal servers and applications and allow for network segmentation to mitigate server vulnerability, as mentioned in this recommendation.

- ***Consider enhancing the passwords security administration process***

  Observation: We noted the current password policy for accounting application is set to expire every six months. We also noted network password policies are setup not to expire.

  Recommendation: We recommend management modify these policies to be in line with industry best practices (approximately 60 to 90 days). Additionally, management should consider implementing a network password policy to ensure against unauthorized access to the network.

  Management response: In 2018, the EAA will update password security policies (network and accounting application) to be consistent in complexity and to have an expiration date of 90 days.

This communication is intended solely for the information and use of management and is not intended to be, and should not be, used by anyone other than this specified party.

RSM US LLP