Finding 2020-001 Information Technology: City-Wide Separation of Duties, Direct Data Changes, and Audit Logging/Monitoring

Significant Deficiency

(Previously partially communicated as findings 2019-001 and 2018-002 as part of the audit of the financial statements for the year ended June 30, 2019 and June 30, 2019, respectively)

Criteria

Statements of Auditing Standards 55 Par 13: Consideration of Internal Control in a Financial Statement Audit: Establishing and maintaining an internal control structure is an important Management responsibility. To provide reasonable assurance that an entity's objectives will be achieved, the internal control structure should be under ongoing supervision by Management to determine that it is operating as intended and that it is modified as appropriate for changes in conditions.

Internal controls over financial reporting are reliant on information IT controls which are designed effectively. In that regard, an effectively designed IT environment is one where an organization maintains the following:

Separation of Duties – the organization documents separation of duties of individuals and defines information system access authorizations to support separation of duties. Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.

*Least Privileg*e – the organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Access Restrictions for Change – the organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Organizations should maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes.

Audit Events – the organization:

a. Determines that the information system is capable of auditing organization-defined auditable events;

b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and,

d. Determines that the organization-defined audited events are to be audited within the information system along with the frequency of (or situation requiring) auditing for each identified event.

Audit Review, Analysis, and Reporting – the organization reviews and analyzes information system audit records periodically for indications of inappropriate or unusual activity and reports findings to the appropriate personnel or role within the organization. Information security-related auditing performed by organizations can include, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP.

Condition

Grant Thornton team met with individual system owners and points of contact to discuss the nuances of these findings which varied slightly based on information system use, architecture, and other factors.

Account Management controls must be used to limit system activities to ensure legitimate use and least privilege. Access controls provide assurance that critical systems assets are safeguarded and that logical access to sensitive applications, system utilities, and data is provided only when authorized and appropriate. Further, broad or special (privileged) access privileges, such as those associated with operating /database system software, administrative accounts, and /or superusers, may allow normal controls to be overridden or otherwise circumvented. Additionally, a lack of logging and monitoring broad or privileged access may result in unusual or suspicious activity going unidentified. Management should address the following:

<u>Separation of Duties</u>

Grant Thornton noted that system access was provisioned based on the supervisor's request and approval from each relevant financial department. However, Management has not developed and documented guidance relating to separation of duties for one system tested to define conflicting role combinations for the system that should be enforced during the account provisioning process.

<u>Direct Data Access</u>

Grant Thornton noted that although direct database changes are rarely required within FMS, the Toad software database for Oracle Database Management tool enabled administrative users of the tool the ability to modify or make direct changes to production data within the database. It has been explained by management that privileged users were required to obtain approval before making changes to data via the Toad tool, however, systematic restrictions were not in place to require an approval prior to direct data updates being made and logging was not active on the database to enable monitoring of the activities of privileged users (e.g. direct data changes).

Context

IT general controls (ITGC) are the first layer of information system controls and are applicable entity-wide at the network, operating system and infrastructure level. The objective of ITGCs are to ensure proper development and implementation of applications, as well as the integrity of programs and data across the organization. Control deficiencies at the ITGC level can lead to ineffective controls at the application level.

Cause

Management has not implemented a policy and procedures that appropriately document account management requirements as part of their internal control framework. Management has not defined requirements for privileged user accounts and logging/ monitoring in policy and procedures.

Effect

<u>Separation of Duties</u>

Failure to effectively restrict access to applications based on job function and employ adequate separation of duties increases the risk for abuse of system privileges, fraud, and inappropriate activity without collusion.

<u>Direct Data Access</u>

Direct data changes bypass system transactions and controls and therefore increase the risk of inappropriate updates to data. This may impact the organization’s ability to rely on the completeness, accuracy, and validity of data. Further, without monitoring processes in place, there is no accountability or secondary validation that the privileged user's activity was authorized and/or appropriate. These issues may result in unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems, which may lead to misstatements on the financial statements. Further, the use of shared user accounts on a production system reduces the audit and accountability of users within the system and password security. In other words, there is no traceability of user's activity to perform these changes to production data.

Recommendation

We recommend that Management:

- Design and document separation of duties matrices to assist system users, supervisors, and system administrators to request and grant the appropriate level of access based on the users' roles and responsibilities.

  - Analyze the risk of allowing certain users the capability to make direct changes to the database without compensating controls in place.

- Implement controls to systematically restrict data changes without approval, to generate alerts when data is changed, and/or to actively log and monitor the use of the tool to change data or system parameters.

Office of Retirement Services Response (unaudited)

As this recommendation is directed toward City-wide IT controls, ORS is limited to what it can do. ORS must adhere to central IT's policies and procedures. Therefore, any changes to their processes are rolled out from the City. ORS' IT division is informed of any changes to their policies via emails and meetings with Central IT, which is then disseminated throughout ORS.

In addition, ORS has implemented policies and procedures to ensure a separation of duties so that any inappropriate activities can be detected. Controls are in place to review/audit updates made by staff members. Any updates to members' records that do not have supporting documentation for the update is followed up on by IT management. In addition, there are a total of 28 users in the PensionGold system, for which access is reviewed when there are any staff position changes (i.e. change in roles or responsibilities and when there are any staff position changes (i.e. change in roles or responsibilities and when there are new staff hired or terminated).

Finding 2020-002

GASB No. 72 Fair Value Measurement Disclosure

Significant Deficiency

(Previously communicated as part of finding 2019-002 in connection with the audit of the System's financial statements for the year ended June 30, 2019)

Criteria

Statements of Auditing Standards 55 Par 13: Consideration of Internal Control in a Financial Statement Audit: Establishing and maintaining an internal control structure is an important management responsibility. To provide reasonable assurance that an entity's objectives will be achieved, the internal control structure should be under ongoing supervision by management to determine that it is operating as intended and that it is modified as appropriate for changes in conditions.

Condition

Reclassification adjustments related to the GASB Statement No. 72, *Fair Value Measurement and Application* (GASB 72) leveling disclosures were identified during the audit process in the System's financial statements. An appropriate detailed review of the investments in each level category was not completed at the appropriate level of precision to identify any misclassifications in the different fair value categories, as required under the definitions of US GAAP.

Context

As required by fair value standards provisioned by GASB 72, analysis is required by management to develop a process of internal validation of valuations provided by Managements' specialists. This broadly would require a timely and precise review and understanding of the methods used by the custodian and investment managers to measure fair value and to undertake periodic validation of the amounts provided by those parties, as well as determining correct levelling disclosures.

Cause

Management had not implemented a precise level of final review to classify the investments to their appropriate leveling category, as defined in GASB 72, in a timely manner.

Effect or Potential Effect

The fair value investment disclosures that are required to be reported, particularly the levelling and NAV disclosures, are potentially inaccurate and incomplete. Delays in management's collective efforts to obtain an understanding of the nature of each investment to determine correct levelling and NAV disclosures results in the financial statements and related disclosures being prepared incorrectly.

The audit process identified certain securities classified by management as level 1 that were not supported by objective evidence of an observable quote price. The valuation process utilized by the auditors indicated these should be classified as alternative (or

NAV) or level 2 investments. Additionally, the audit process identifies inconsistencies in leveling between the trusts and plans. As a result, the entire portfolio had to be reassessed by management for correct levelling disclosure which consisted of understanding the underlying investments and ensuring consistent leveling between the trusts and plans; a process that should have occurred prior to the audit commencement.

Recommendation

We recommend management:

- Develop and implement a periodic review and levelling categorization of each of the investments throughout the fiscal year, to remain cognizant of any changes in valuation assumptions or matters that may cause a change in levelling disclosures.
- Develop and implement a timely, robust and comprehensive review of the investments collectively with information required from the Investments team and review/determination from the Accounting team, as required for annual financial reporting for the disclosed leveling categories.

Office of Retirement Services Response (unaudited)

Management has implemented additional measures to ensure that the leveling is accurate. After the Investments group provides the leveling for each security, the Accounting group will compare each security from one plan to the other, as well as to prior year to ensure that the leveling is consistent throughout. A master leveling security list was compiled to assist with the review process, and an additional staff person was added to the review process to allow for four levels of review in the Accounting group.