IT General Controls

Phase 1

Internal Audit Report

May 25th, 2023

Orange County Public Schools
Internal Audit

Linda J. Lindsey, CPA, CGAP, School Board Internal Auditor
Luis E. Aponte Santiago, CISA, Senior Internal Auditor

Table of Contents

EXECUTIVE SUMMARY

Why We Did This Audit

The objective of this audit was to developed an assurance that the IT general controls for the district are reliable, efficient and effective. This is the first of four planned audits related to IT general controls.

This audit report covers the following topics: Information Security Management, Network Infrastructure and Environmental Exposures & Physical Access.

This audit was included in the 2021-2022 Annual Audit Plan.

Observations and Conclusion

Audit Results at a Glance			
	Risk / Impact Rating		
Results and Observations	Significant	Moderate	Minor
Source IA - Internal Audit or M - Management	IA - 1	IA - 1	IA - 1
Observation Category D - Deficiency or O - Opportunity	D - 1	D - 1	D - 1

The district has written policies, procedures and standards regarding ITS operations. We also noted logical access security measures were in place and formal security awareness training was provided.

In addition, the duties of a Security Administrator are executed; documentation of new IT users, data users and other authorizations are developed; terminated employees and third-parties are withdrawn from the system promptly; and documentation such as network diagrams, policies, roles & responsibilities, are in place for most components of the network, among many other tasks.

Results and Recommendations

We made the following recommendations to the district regarding situations we found within the areas of Information Security Management; Network Infrastructure Security; Environmental Exposures and Physical Access:

- Update the Change Management Process document.
- Document that follow-up actions from Network Penetration Tests have been performed.
- Renew Remote Access forms in a timely manner.

This report has been discussed with management and they have prepared their response which follows.

DEFINITIONS:

Risk / Impact Ratings

Minor	Low risk with a financial impact of less than one percent and/or an isolated occurrence limited to local processes (low impact and low likelihood)
Moderate	Slight to moderate risk with a financial impact between one and five percent and/or a noticeable issue that may extend beyond local processes (low impact and high likelihood or high impact and low likelihood)
Significant	High risk with a financial impact greater than five percent and/or a significant issue that occurs in multiple processes and/ or noncompliance with Florida Statutes or School Board Policies (high impact and high likelihood)

We categorize risk/ impact as:

- *Minor*
- *Moderate*
- *Significant*

Observations Categories

Opportunity	A process that falls short of best practices or does not result in optimal productivity or efficient use of resources
Deficiency	A shortcoming in controls or processes that reduces the likelihood of achieving goals related to operations, reporting and compliance

We categorize our observations as opportunities or deficiencies.

Criteria for Observations Sourced to Management

- Internal audit was informed of the issue prior to starting detailed testing
- Management identified, evaluated, and communicated the issue to appropriate levels of the district
- Management has begun corrective action with clear, actionable plans and targeted completion dates

None of these findings were sourced to management.

BACKGROUND:

IT General Controls (ITGC) are defined as controls which relate to the environment within which computer-based application systems are developed, maintained and operated, and which are therefore applicable to all applications. The objectives of general controls are to ensure proper development and implementation of applications, integrity of program and data files, and of computer operations. Like application controls, general controls may be either manual or programmed. Examples of general controls include development and implementation of an IS strategy and an IS security policy; organization of IS staff to separate conflicting duties and planning for disaster prevention and recovery.

Objectives of general controls are to ensure proper development and implementation of applications, integrity of programs and data files, and of computer operations.

The last IT General Controls audit we performed was in 2015. That audit addressed:

- IT Organization
- IT Administration
- Enterprise Architecture
- IT Strategy; Systems Development and Maintenance
- IT Security; Data Center Operational
- Support Services.

As of June 19th, 2023, the ITS department consisted[1] of the following:

- 132 employees
- Six sub-departments[2]
- 31 contractors or consultants

This audit will be conducted in four phases as described under "Methodology" below. This report is for the first phase. Reports will be issued for the other phases as they are completed.

This audit is being conducted in four phases. This is the first phase.

[1] This information was gathered from a questionnaire sent to the ITS Department during the planning phase of the audit and was updated during the course of the audit.

[2] ITS Administration, Business Operations, Information Security, ITS Operations (Infrastructure), SAP Basis Business Systems and Student Information Systems.

OBJECTIVE, SCOPE AND METHODOLOGY:

Objective

The objective of this audit was to determine whether IT general controls are reliable, efficient and effective.

Scope

The scope of the audit was based on the following control topics:

- Information Security Management
- Network Infrastructure Security
- Environmental Exposures and Physical Access Controls
- Mobile Computing
- Cloud Computing
- Data Leak Prevention or Data Loss Prevention
- Information Systems Operations, Maintenance and Service Management
- Applications Control and Incident & Problems Management.

Our scope included ten control topics.

This audit did not include a review of the ITS Governance Framework because it was addressed in the Data Governance Audit in June, 2020. Because the ITS department does not develop applications, Systems Development and Maintenance procedures did not need to be addressed.

ITS Governance was addressed in our Data Governance Audit in 2020.

Methodology

We conducted this audit in accordance with the *International Standards for the Professional Practice of Internal Auditing* of the Institute of Internal Auditors and included such procedures as deemed necessary to provide reasonable assurance regarding the audit objective. Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

We conducted this audit in accordance with the International Standards for the Professional Practice of Internal Auditing.

We are required to note any material deficiencies in accordance with Florida Statutes, School Board Policy and sound business practices. No material deficiencies were noted in this audit. We also offer suggestions to improve controls or operational efficiency and effectiveness.

No material deficiencies were noted in this audit.

We performed audit procedures to determine what controls exist to prevent material errors or irregularities, and whether they are effective. Also, we were alert to indicators of fraud. Specifically, we performed the following tasks:

- Interviewed personnel from the ITS department, contractors and consultants (when applicable).
- Compiled and reviewed documentation associated with the General Controls being audited.
- The audit programs were created based on the *ISACA's CISA Manual 26th Edition Chapter 5 – Protection of Information Assets*.
- Tested controls and procedures related to established methodologies and practices for the IT General Controls mentioned on the scope of the audit. We had an audit test to determine whether proper physical and logical access controls were in effect and to inventory the various terminal connections to ensure that diagram is accurate was not assessed because the district's network is setup in a way that it only tracks user credentials instead of devices.
- Evaluated the results of the controls tested, draw conclusions and issue recommendations (if any).

The audit programs for this audit were based on Chapter 5 form the ISACA's CISA Manual 26th Edition.

We are conducting the audit in four (4) phases. At the end of each phase, we will issue an audit report that will be discussed with district management. The topics for each phase are:

- Phase 1 - Information Security Management; Network Infrastructure Security; Environmental Exposures and Physical Access
- Phase 2 – Mobile Computing; Cloud Computing and Data Leak Prevention or Data Loss Prevention
- Phase 3 – Information Systems Operations, Maintenance and Service Management
- Phase 4 – Applications Control and Incident & Problems Management

This IT General Controls Audit is being conducted in four (4) phases.

RESULTS & RECOMMENDATIONS:

Overall Conclusion: Our overall conclusion is that the district has written policies, procedures and standards regarding ITS operations. We concluded logical access security measures were in place and formal security awareness training was provided. We also noted the following aspects of the ITS department's IT general controls:

- The duties of a Security Administrator are executed.
- Documentation of new IT users, data users and other authorizations are developed.
- Terminated employees and third-parties[3] are withdrawn from the system as early as possible.
- A baseline security plan for IT activities is in place along with access standards.
- Documentation, such as network diagrams, policies, roles & responsibilities, are in place for most components of the network.
- Remote access is documented.
- A Network Penetration Test (NPT) was performed
- Development and authorization of network changes are documented and environmental exposures and physical access controls for the main computer sites (data centers) are addressed.

We noted three (1) minor, one (1) moderate and one (1) significant situations that need to be addressed. Our detailed findings and recommendations follow.

Our overall conclusion is that the district has written policies, procedures and standards regarding ITS operations.

[3] Contractors and/or consultants.

1) Update the Change Management Process document[4] to reflect current department name, position titles and functions.

Minor (Risk or Impact) Deficiency

Best Practice:

Vital documentation should be current. Department names, position titles, and functions should reflect current organization structure and personnel.

Vital documentation should be current.

Audit Result:

When we read the Change Management Process document, we noted discrepancies in its title[5], the positions on the Change Management Review Board, and the name of the review board[6]. The name and the roles of persons that comprise this board have changed. According to documentation provided by the ITS department, the Change Management Review Board is now called the Change Advisory Board (CAB) and its members are two (2) Assistant Directors for ITS and a Sr. Manager for ITS.

The Change Management Process document did not reflect current information and should be updated.

Recommendation:

We recommend the ITS department update the Change Management Process document to reflect the current department name, add the current job position names in the Change Management Review Board under Change Management Roles, and change the name of the Change Management Review Board to "Change Advisory Board."

2) Document the follow-up actions from the Network Penetration Test (NPT) recommendations.

Significant (Risk or Impact) Deficiency

Best Practice:

According to Core Security, it is important to conduct a post-mortem to disseminate, discuss, and fully understand NPT findings. With review

[4] Verbal recommendation.

[5] The current title is Information, Communications and Technology Services (ICTS) Change Management process. The department's name is now Information Technology Services.

[6] The review board is now called the Change Advisory Board.

and evaluation, pen test results can transform into action items for immediate remediation and takeaways that will help shape larger security policies. The important action items to consider after completing an NPT include:

- Review and Discuss the Pen Test Results
- Develop a Remediation Plan and Validate Implementation with a Retest
- Incorporate Findings into Your Long-Term Security Strategy

Audit Result:
We asked ITS Senior Leadership whether there was a follow-up on the results of the NPT and they responded that a report was made. To validate this information, we requested said report of ITS Senior Leadership and they told us that us a review was made by the former CIO. When we asked for notes or other evidence of his review, we were told none were available. There was no evidence of this review or of specific follow-up actions he directed to address the NPT results.

It is important to conduct a post-mortem to disseminate, discuss, and fully understand the findings of a Network Penetration Test.

Recommendation:
We recommend the ITS department perform and document follow-up actions taken to address the results of an NPT. These actions could include developing a remediation plan to address the NPT findings, validating whether the changes made resolved those NPT findings, and revising continuous monitoring efforts as appropriate.

3) Renew Remote Access forms in a timely manner.

Moderate (Risk or Impact) Deficiency

Best Practice:
According to Section NIST Special Publication 800-46r2, Section 3.3 Remote Access Authentication, Authorization, and Access Control, most of the computing resources used through remote access are available only to an organization’s users, and often only a subset of those users. To ensure that access is restricted properly, remote access servers should authenticate each teleworker before granting any access to the organization’s resources, and then use authorization technologies to ensure that only the necessary resources can be used. Authentication can also be used to confirm the legitimacy of telework client devices and

remote access servers. Access control technologies are also needed to restrict access to network communications and applications. This section provides additional details on remote access authentication, authorization, and access control.

Audit Result:
The remote access form for two (2) contractors were signed on the day the ITS department responded our information request[7]. The district's Consultant Network Use Agreement states that the form is required for all non-OCPS employees that require a district e-mail account and network logon to perform their duties. Expiration dates are set and accounts must be renewed prior to any computer network or Internet usage.

Two (2) contractors' remote access authorization forms were signed the day of our request although they had already been working with the district for approximately six months.

Recommendation:
We recommend the district verify all contractor's remote access forms in a timely so they can renew the ones that needs to be renewed.

We wish to thank the personnel from the ITS department (including contractors) and all the other departments that were involved in this audit for their cooperation and assistance we received through the course it.

[7] December 16th, 2022.

AUDIT RESPONSE MATRIX FISCAL PERIOD OR AUDIT DATE: 08/01/2023

Department / School Name	**ITS**
Administrator / Department Head	**John A. Davis**
Cabinet Official / Executive Leader	**Aaron Ross, Russell Holmes, Amy Abner**

Audit Result / Recommendation	**Management Response Acknowledgement/ Agreement of Condition**	**Responsible Person (Name & Title) And Target Completion Date**	**Management's Action Plan**
Update the department's name and information within the Change Management Process document.	Management agrees with the recommendation.	**Aaron Ross, Sr. Director Business Operations** **8/2023**	Evidence was provided to Internal Audit, in the form of the *Change Enablement Process* document, on 7/17/23 documenting the requested changes.
Document follow-up actions after the Network Penetration Test (NPT) was performed	Management agrees with the recommendation.	**Russell Holmes, Sr. Director Information Security** **06/2024**	ITS intends to implement a yearly NPT, and is currently working with a vendor to complete a Pen Test for the 23-24 fiscal year. ITS is also working with Procurement to secure a simple vendor selection process in order to easily accomplish NPT's in future years.
Renew remote access forms in a timely manner	Management agrees with the recommendation.	**Amy Abner, Sr. Director SAP Basis, Business Systems** **12/2023**	To mitigate this issue in the future, ITS is going to fully automate this process in Easy Vista. Thereby having electronic approvals of this type readily available.