Data Center Audit

Internal Audit Report

October 18, 2019

Orange County Public Schools

Internal Audit

Linda J. Lindsey, CPA, CGAP, Senior Director
Luis E. Aponte Santiago, CISA, IT Internal Auditor

Table of Contents

EXECUTIVE SUMMARY

Why We Did This Audit

Due to new emerging technologies in the IT field and cost-savings initiatives, OCPS decided to move their data center services to an off-premises facility that does most of the related tasks. This affected our risk assessment and we audited to provide assurance related to the new data center.

This audit was included in the 2019-2020 Annual Audit Plan.

Observations and Conclusion

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

Overall, the District made a sound business decision in moving most of their data center activities to an off-premise location managed by a third-party that is solely dedicated to this type of service. The primary controls outsourced to them are physical security, power availability and environmental concerns.

Results and Recommendations

- Request, read and review the colocation site's annual SOC report in a timely manner to obtain assurance on their physical and security measures in place and compensating controls that we need have in place. Monitor vendor performance by obtaining these reports annually.

- Have the consultant's "Access Grantor" access revoked, so that he is not able to open temporary access requests and permit guests or vendors access to our colocation suite without our knowledge.

They need to address the issue of requesting the third-party vendor their Service Organization Controls (SOC) 1 or 2 Reports.

This report has been discussed with management and they have prepared their

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 (high impact and high likelihood)

Observations Categories

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

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 the observations resulting from this audit made were sourced to management.

BACKGROUND:

Due to new emerging technologies in the IT field and cost-savings initiatives, OCPS decided to move their data center services to an off-premises facility that does most of the tasks.

OBJECTIVES, SCOPE AND METHODOLOGY:

Objectives

The objectives of this audit were to provide assurance on OCPS' outsourced data centers on the following:

- All sites meet OCPS' availability and reliability needs.
- OCPS equipment is secure and safe from known environmental hazards and technological threats.
- Third-party agreements (Master Service Agreements, Service Level Agreements, Acceptable Use Policy, Partnerships agreements and others, if any that applies) with DataSite and DSM Technologies Consultants, LLC are properly examined and vetted.
- Appropriate contractual provisions regarding the services provided by DSM Technologies Consultants, LLC to OCPS.
- Appropriate physical and logical controls in OCPS environment.

The audit addressed assurances related to the outsourced data center.

Scope

The scope of the audit included colocation services for the primary operating data center in Orlando as existed during FY 2018-19.

Our scope included colocation services for the primary operating data center in Orlando as existed during FY 2018-19.

Methodology

Our audit was conducted 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.

This audit was conducted 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. We also offer suggestions to improve controls or operational efficiency and effectiveness.

In performing this audit we:

- Conducted interviews with ITS Department and vendor (DataSite)
- Visited the colocation to see if it complies with regulations and standards.
- Reviewed formalized contract for the colocation site
- Reviewed and analyzed the SOC 1 Report from DataSite
- Reviewed regulations, policies and procedures such as:
    a. NIST 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
    b. DSM Technologies' Service Level Agreements (SLA), Master Service Agreement (MSA) and Acceptable Use Policy
    c. DataSite's Colocation Service Guide and Data Center Policies

COMMENDATION:

The District made a sound business decision on moving most of their data center activities to an off-premises location. With this strategic movement, it shifted most of the risks and regulatory compliance issues associated with this type of asset away from our daily routine to a third-party vendor for which these are core business practices.

With this strategic movement, it shifted most of the risks and regulatory compliance issues associated with this type of asset away from our daily routine to a third-party vendor for which these are core business practices.

We did a walkthrough of their facilities and we could attest that the facility is well kept, from power efficiency to physical security measures and environmental controls.

RESULTS AND RECOMMENDATIONS:

1) The ITS Department did not verify the colocation site's physical and security measures by obtaining their Service Organization Control (SOC) Report[1] before engaging in a contractual agreement
Significant Risk / Internal Audit

[1] For our audit, we requested DataSite Orlando SOC report. The district's data center at DataSite Atlanta (OCPS Hot Site for Disaster Recovery) was not included in this audit scope.

Best Practice:

Obtaining a SOC report before engaging in a contractual agreement with a third-party organization provides:

- independent assurance regarding the controls operated by that vendor;
- clearly articulated complementary controls that need to be performed by us in order to achieve certain control objectives;
- a comprehensive report of the process and controls in place; and
- insight into control gaps highlighted in the report

Perform due diligence prior to entering an agreement by obtaining and reviewing SOC report to evaluate vendor controls.

Audit Result:

As per the management team of the colocation site, they make sure all physical and security measures are tested by doing a 6-hour complete walkthrough on their facility every day. However, the ITS Department didn't require the vendor to provide, at least, a SOC report to verify that their physical and security measures were being tested before they engage in a contractual agreement, therefore putting at risk a District's key asset[2]. The first SOC report received by the District was in response to our request during this audit.

Recommendation:

Request, read and review the colocation site's SOC report on an annual basis for the term of the contractual agreement to obtain assurance of their physical and security measures and the compensating controls that the district needs to have in place in order to achieve certain control objectives.

Request, read and review the colocation site's SOC report on an annual basis for the contractual agreement so OCPS can have assurance of their physical and security measures and the compensating controls that we need to take care of in order to achieve certain control objectives.

2) An external consultant had "Access Grantor" authority on the colocation site Access Client List *Minor Risk / Internal Audit*

Best Practice:

Add the column "company" or differentiate between internal or external resource on the Customer Access List, so it would be much clearer to determine the type of access each person has.

[2] Data Center activities and related tasks.

Audit Result:

An external consultant had the "Access Grantor" type access on Client Access List. According to DataSite management, this type of access is able to open up a temporary access request to permit guests or vendors access to the OCPS colocation suite.

Recommendation:

Have the external consultant's access grantor access revoked, so that he's not able to open up temporary access requests and permit guest or vendors access to our colocation suite without OCPS knowing.

Have the external consultant's access grantor access revoked, so that he is not able to grant temporary access requests and permit guests or vendors access to our colocation suite without OCPS knowing.

We wish to thank the ITS management and staff for their cooperation and assistance in this audit.

MEMORANDUM

ITS
Chief Information Office

Date: November 7, 2019

To: Linda Lindsey, Sr. Director, District Internal Auditor

From: Robert Curran, Chief Information Officer

Subject: Management Response to Recommendations for the Data Center Audit report

Recommendation 1: Request, read and review the colocation site's SOC report on an annual basis for the term of the contractual agreement to obtain assurance of their physical and security measures and the compensating controls that the district needs to have in place in order to achieve certain control objectives.

Management Response: The SOC report has been reviewed and will annually be requested and reviewed.

Recommendation 2: Have the external consultant's access grantor access revoked, so that he's not able to open up temporary access requests and permit guest or vendors access to our colocation suite without OCPS knowing.

Management Response: The consultant's access has been removed.