IT Security Assessment Follow-Up

Internal Audit Report

June 18, 2021

OCPS Orange County Public Schools

Internal Audit

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

Table of Contents

EXECUTIVE SUMMARY

Why We Did This Audit

Our objectives for this audit were to determine that relevant recommendations from the previous security assessment [1] were implemented and determine what has been done to complete the recommendations; to evaluate the contractor's services and compare them to best practices and internal capabilities and evaluate the current IT security posture.

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 – 0	IA – 1	IA – 1
D - Deficiency or O - Opportunity	D – 0	D – 1	O – 1

Our overall conclusion is that the ITS department was able to identify relevant recommendations from the previous IT Security Assessment and address the risks of those by implementing action plans consisting of various application tasks and using an identity service engine to segregate the network.

With the help of a contractor, the ITS department has developed and implemented a security plan to address the risks that the IT environment faces every day and the District was engaging appropriately with qualified personnel to manage their security program.

However, we noted opportunities for improvement as described below.

Results and Recommendations

We recommend that:

The ITS department complete the mitigated vulnerabilities report that includes the alert date, CVE number, CVE name, host, risk, solution, district's mitigation date and patch mitigation date.

Prior to signing any contract, discuss with the contractor any expectations the ITS department has and be certain the formal agreement contains exactly the tasks preliminarily agreed upon and how they will be accomplished.

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

[1] Performed by a third-party on September 2018.

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 and 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:

This is a follow-up engagement to the Information Security Assessment performed in September 2018.

In 2016, management's risk assessment indicated a risk of the potential for email accounts to be subject to harvesting / scraping / phishing by spammers. As a result, we determined to perform penetration testing in collaboration with the ITS department in order to establish a baseline understanding of our email system's security status. After discussion and analysis of the existing circumstances, the Chief Information Officer (CIO) and the Chief Audit Executive (CAE), with support of the Audit Committee and input from the Senior Director of IT Security at that time, it was agreed that a more comprehensive assessment of cybersecurity was needed. Accordingly, the 2017 audit plan replaced the email security audit with a comprehensive IT security audit which was outsourced.

The audit included penetration testing and much more.

The objective of the 2018 audit was to establish a baseline determination of the (then) current status of our IT security program and its vulnerabilities and develop recommendations for improving it.

After the 2018 audit, the ITS department entered an agreement with a contractor. The agreement contains two separate statements of work (SOW): (1) CISO[2] as a Service and (2) Managed Security Services. Each SOW has separate tasks. In summary, those tasks consisted of the following:

- The contractor performs vulnerability scans, which the ITS Security Team evaluates and notifies the business owners or act on themselves;
- 24/7 eyes on the network allowing for calling district staff for critical alerts after hours, minimizing adverse impacts; and
- Notifications of security concerns such as patches or other security concerns that we may not currently know exist.

This was a follow-up to a previous security assessment performed in 2018.

The objective of the 2018 assessment was to establish a baseline determination of the (then) current status of our IT security program and its vulnerabilities and develop recommendations for improving it.

ITS has engaged a contract CISO and outsourced its Managed Security Services.

[2] Chief Information Security Officer.

OBJECTIVES, SCOPE AND METHODOLOGY:

Objectives

The objectives of this audit were the following:

1) Determine whether relevant recommendations relevant to the ITS from the previous security assessment[3] have been implemented;

2) Determine what's been done to complete the recommendations;

3) Evaluate contracted services and compare them to best practices and internal capabilities; and

4) Evaluate the current IT security posture.

These objectives are divided into two audit programs: *IT Security Assessment Follow-Up Audit Program* and *Contractor's IT Security Function Audit Program*.

We evaluated:

- *progress in addressing recommendations from the 2018 audit*
- *contracted services*
- *current IT security posture*

Scope

The scope of the audit was the status of the ITS department's security program as of January 2021.

Our scope was the status of the ITS department's security program as of January 2021.

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.

We noted no material deficiencies during this audit.

[3] Performed by RSM in 2018.

Our audit methodology consisted of the following:

- Interviewing ITS personnel and contractors to gather information regarding their experience and knowledge in the information security field;

- Documenting and evaluating policies, procedures and processes in regards with information security;

- Evaluating the ITS department's security needs and what a contractor offered the district with the signed statements of work (SOW) with their deliverables, Service Level Agreements (SLA) and performed tasks; and

- Testing controls, procedures and strategies by selecting various samples related to the ITS security program/mitigation plan.

<u>RESULTS & RECOMMENDATIONS:</u>

<u>Overall Conclusion:</u> Our overall conclusion is that the ITS department determined that the recommendations for applications and for network areas from the previous IT Security Assessment were still relevant. They have prepared action plans to address the risks that they present to the current environment. The plans include the following:

- Application: update - create a mitigation plan so the application can become an "island"[4] or shut it down

- Network - they will use an identity service engine (ISE) to segregate the network. This project will be completed in approximately 1 ½ years.

The ITS department determined the recommendations that were still relevant and prepared action plans to address the risks that they present to the current environment.

For the current IT security posture, they have a security plan in place. With the help of a contractor, the ITS department has developed and implemented a security plan to address the risks that the IT environment faces every day. The security plan consists of real-time vulnerability scans performed by the contractor, which are then mapped into a report that they create using the Power BI tool. The report has an overview with the following categories:

The security plan consists of real-time vulnerability scans performed by the contractor, which are then mapped into a report that they create using the Power BI tool.

[4] Meaning to give access only to the personnel that need it.

- Overall Rating, Access Control; Awareness & Training, Backup Management, Device Management, Email Security, Endpoint Security, Password Weakness and Vulnerability Management.

We evaluated both the contractor's and the district's personnel, and compared them to best practices and internal capabilities. We were able to determine the district was engaging appropriately qualified personnel to manage the security program.

Both the contractor's and the district's personnel are qualified to manage the security program.

Our detailed findings and recommendations follow.

1) Complete the mitigated vulnerabilities report. ***Moderate Risk***

Best Practice:

If we're going to rely on a document or report[5] which tells the district's ITS security team the type and risk of the vulnerability that was found, where it was found[6] and the solution to mitigate or eradicate it, it will be also beneficial for the district to have a document or report where these vulnerabilities can be mapped with their respective mitigation dates. This will be helpful in the following:

- History of all mitigated vulnerabilities by the district;
- Tracing back the mitigated vulnerability if it is found in subsequent months (mitigated in January but is reported again in May); and,
- Useful for future infrastructure decisions (i.e.: if a vulnerability is commonly found in devices with certain OS or a certain brand, we can avoid purchasing those and select the less "vulnerable" to those. Also, selection could be based depending on the risk, device and district's risk appetite, among many other things).

Audit Result:

During the audit, we analyze the latest vulnerability scan[7] and found that the report has, among many other things, the following attributes:

The ITS department did not have a report for mitigated vulnerabilities with information such as when the vulnerability was mitigated.

[5] Vulnerability scan

[6] Host

[7] January 2021

- CVE[8] number, vulnerability name, host, risk, synopsis, description and solution.

We asked the ITS Senior Director of Information Security if the vulnerabilities in the report had been mitigated and if so, how long it took the district to mitigate them. He told us that they don't have a document or report with that information, but that they were working on it. In other words, the vulnerabilities can't be mapped or traced to verify if they have been closed because that information has not been gathered yet.

A record of mitigated vulnerabilities will assist in tracking progress and verifying mitigation actions.

As of today, the only way to know if any vulnerabilities have been mitigated is to do a monthly comparison of the vulnerability scans and map which vulnerabilities from the previous report are not on the most recent report. But this will not include mitigation dates.

<u>Recommendation:</u>
Complete the mitigated vulnerabilities report including the following attributes:

- Alert date[9], CVE number, CVE name, host, risk, solution[10], district's mitigation date and patch[11] mitigation date.

This can be done by incorporating tools like Power BI and other alternatives. The benefits of having a report of mitigated vulnerabilities can vary, but would include having information on the vulnerabilities like days from discovery to mitigation, days without being mitigated, and concurrent vulnerability (by host, by IP, etc.) among many others.

2) Address desired expectations of an agreement in a clear and direct manner. *Minor Risk*

Contracts should contain a clear description of the work expected to be performed.

<u>Best Practice:</u>
The vendor is required to perform or deliver what is agreed upon in the contract, emphasizing on all the items that the District has categorized

[8] Common Vulnerabilities and Exposures
[9] Date where the vulnerability was found (maybe on the vulnerability scan)
[10] This could the actual solution or any workarounds
[11] If patch is made and is available

as high-risk or important. If the contract is not clear or does not contain all these items, the vendor may not perform them. Additionally, it is the District's responsibility to ensure that these high-risk or important items are included in the contract.

Audit Result:

During the audit, we asked the ITS department their expectations of the contractor in the SOW's and they told us the following:

- Complete the Risk Assessment, conduct a Business Impact Analysis, conduct a tabletop exercise, work on an updated Disaster Recovery Plan (DRP) and email phishing campaigns.

We noted that most of the ITS department's expectations for the contractor were not included as tasks in the SOW's.

After evaluating both SOW's[12], we determined that only two of the five department expectations were included in the signed agreement. We found some indications about the email phishing campaigns[13] that could be included in item #15 of the CISO as a Service SOW day to day activities, but that was not very clear.

Item #15 on the SOW day to day activities stated that the CISO is responsible for coordinating the completion of OCPS' annual cybersecurity risk assessment to include provisioning of remediation recommendations. This activity shall include assisting the district in determining its Cybersecurity Maturity Levels necessary to develop a roadmap of activities required to elevate these levels.

Fortunately, the contractor is currently providing the services expected by management. But were the contractor to perform only to the written letter of the contract document, the district's needs would not be met.

Recommendation:

Prior to signing any contract, discuss with the contractor any expectations the department has and be certain the formal agreement contains exactly the tasks preliminarily agreed upon and how they will be accomplished. This will reduce the risk that critical tasks will not be performed, and will avoid changes to the agreement for tasks that were left out, thus saving economic resources for the District.

The ITS department should include all their expectations in the form of tasks in the signed agreement.

[12] CISO as a Service and Managed Security Services.

[13] The contractor is performing this task every month.

We wish to thank all the ITS Department personnel and the ITS Information Security Team (including contractors) for the cooperation and assistance we received in the course of this audit.

AUDIT RESPONSE MATRIX FISCAL PERIOD OR AUDIT DATE: 2020-2021

Department / School Name	**ITS, Information Security**
Administrator / Department Head	**Russell Holmes**
Cabinet Official / Area Superintendent	**Robert Curran**

Audit Result / Recommendation	**Management Response Acknowledgement/ Agreement of Condition**	**Responsible Person (Name & Title) And Target Completion Date (MM/YYYY)**	**Management's Action Plan**
Complete the mitigated vulnerabilities report.	ITS Agrees that documenting critical vulnerabilities and mitigation is essential.	Russell Holmes August/2021	We already have this in place for EoL/EoS Operating Systems and have already been working to implement a system to monitor and document critical vulnerabilities. We are working on either having an internal tracking mechanism or a system based in our contracted Security Management Dashboard.
Address desired expectations of an agreement in a clear and direct manner.	Management agrees that contractor agreements and contracts should dictate expectations.	Russell Holmes for security related contracts Completion Date: as new contracts are negotiated and needs are identified. August/2021	Contracts in question were created based on needs identified at the time the agreement came into effect. Future needs identified throughout the process were not included as they were identified while conducting assessments with the vendor.