



1000.00
900.00
800.00
700.00

383279
74944
34825
306647
08128

5028841971 6939937510 5820974944
5923078164 0628620899 8628034825
3421170679 8214808651 3282306647
0938446095 5058223172 5359408128



31415926535 8979323846 2643383279
5028841971 6939937510 5820974944
5923078164 0628620899 8628034825
3421170679 8214808651 3282306647
0938446095 5058223172 5359408128



2643383279
320974944
628034825
3282306647
359408128



31415926535 8979323846 2643383279
5028841971 6939937510 5820974944
5923078164 0628620899 8628034825
3421170679 8214808651 3282306647
0938446095 5058223172 5359408128

Table of Contents

Executive Summary	3
Background	3
Objective, Scope and Methodology	3
Issues and Recommendations	4
Observations Table	5
Observations, Recommendations and Management Response	5
1. APS Procurement Policies or Regulations Do Not Address IT Security and Data Risks	5
2. Contract Language Does Not Contain Specific Language to Address IT Security and Data Risks	7
3. A Process for Monitoring Third Parties for IT Security and Data Risks is Not Implemented	10
4. Current Processes Do Not Provide District-Wide Visibility or Oversight of IT Vendors	11

Executive Summary

Rausch reviewed APS policies and procedures governing the purchase of information technology goods and services and found the processes lack specific IT security requirements and activities. Activities to assess or monitor third parties for IT security and data risks during the life of the contract were also not defined nor being performed.

Rausch noted several of the policies and templates are being updated and acknowledges activities are underway by the Procurement team to improve the overall vendor management program including the vendor onboarding process. One relevant improvement noted was the creation of the Software Products and Services Agreement which addresses requirements for the purchase of software and other IT services. Procurement has implemented this in current processes and is securing vendor signatures for existing purchases. We encourage continuation of this effort as well as coordination with IT Security to ensure security and data risks are considered and appropriately addressed.

Based on our interviews, observations, reviews of documentation and review of previous assessments performed, Rausch's evaluation identified four areas for improvement.

Background

Rausch Advisory Services (Rausch) was engaged by the Office of Internal Compliance of Atlanta Public Schools (APS) to complete an Information Technology (IT) Third-Party Management review. Rausch performed the review between February 4, 2020 through March 16, 2020. The executive summary included below summarizes the objectives, scope and observations of the engagement, as well as overall recommendations for APS.

We conducted this audit in accordance with Institute of Internal Auditing (IIA) auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We limited our work to those areas specified in the "Audit Objective, Scope, and Methodology" section of this report.

We used recommended practices and controls identified by ISACA, the National Institute of Governmental Purchasing (NIGP), the Institute for Public Procurement, Principles and Practices of Public Procurement and the NIST Cybersecurity Framework as a basis to compare APS processes.

Objective, Scope and Methodology

The objectives of the IT Third-Party Management review were to provide APS with a high level of assurance that APS had appropriate policies to manage IT Third-Party service providers and performed the necessary monitoring activities to ensure compliance with contractual terms and conditions with respect to managing IT security and data risks.

Rausch did not review the complete procurement process only those activities where IT and IT Security involvement is needed.

To meet our objectives, we reviewed various documents and processes including:

- ✓ APS Procurement Policies and Procedures Manual - 2019
- ✓ APS Formal Solicitation Request Templates
- ✓ APS Regulation - Draft - Oversight of 3rd Party Vendors and Cloud Computing Services
- ✓ APS Regulation – Draft - Administrative Regulation CNA R(2)
- ✓ DJEA Purchasing Authority Regulation
- ✓ FY19-10 Procurement Final Audit Report
- ✓ APS Software Products and Services Agreements
- ✓ APS General Terms and Conditions
- ✓ Contracts for a sample of current vendors providing IT goods or services



The Rausch professional interviewed APS Procurement and IT personnel to gain an understanding of the current processes. The following is a list of interviews we conducted during our review:



- ✓ Executive Director Purchasing
- ✓ Purchasing Agent
- ✓ Procurement Associate (Buyer)
- ✓ Director of IT Security and Network Services

Through the course of the review, Rausch identified gaps within the processes and documented policies and regulations and has provided recommendations to address risk associated with purchasing IT goods and services. This is included in our Findings and Recommendation section below.

Issues and Recommendations

Risk Level Key

-  **High Risk:** matters and/or issues are considered to be fundamental to the mitigation of material risk, maintenance of internal control or good corporate governance. Action should be taken either immediately or within three months.
-  **Medium Risk:** matters and/or issues are considered to be of major importance to maintenance of internal control, good corporate governance or best practice for processes. Action should normally be taken within six months.

-  **Low Risk:** A weakness which does not seriously detract from the internal control framework. If required, action should be taken within 6 -12 months.
-  **Informational:** The identified Informational level findings are not considered risk but may contain valid and useful information that may aid APS with process improvement.

The table below summarizes the observations, the potential risk level and when management anticipates corrective action to be implemented. Detail on the steps required to address the observation is provided in the “Recommendation” section for each item with reference to the corresponding National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) control. APS IT has adopted the NIST CSF Framework.

Observations Table

Number	Observation	Risk Level	Est. Completion Date
1.	APS Procurement Policies or Regulations Do Not Address IT Security and Data Risks	Med	12/31/2020
2.	Contract Language Does Not Contain Specific Language to Address IT Security and Data Risks	High	7/31/2020
3.	A Process for Monitoring Third Parties for IT Security and Data Risks is Not Implemented	High	12/30/2020
4.	Current Processes Do Not Provide District-Wide Visibility or Oversight of IT Vendors	Med	8/31/2020 12/31/2021

The observations of our review along with our recommendations for process improvement with management’s response and implementation timeline are presented on the following pages.

Observations, Recommendations and Management Response

1. APS Procurement Policies or Regulations Do Not Address IT Security and Data Risks

Finding

Rausch noted requirements to identify and assess IT security and data risks when purchasing IT goods and services are not defined in APS Policies or Regulations. While IT is included in some of the processes, specific actions to identify and assess IT security and data risks are not defined. Requirements for assessing the vendor for security risks prior to engagement are not included nor are activities to be performed during the contract period and at termination.

In addition to Procurement Policies, Rausch reviewed a draft of the IT Third Party Oversight Regulation, CNA-R2, proposed by IT Security. The initial draft did address many of the needed items; however, many

were removed from the current draft. Key components that were omitted include conducting information security assessments, receiving third party attestations for IT service providers, and defining minimum security requirements for third parties to follow.

Risk

Potential and realized IT security and data risks may not be known or addressed.
Selected third parties may not be capable of protecting APS data.

Recommendation

NIST CSF Control: ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.

Rausch recommends APS include cyber supply chain risk management requirements in District-wide Procurement Regulations and Policies. These Regulations or Policies should identify the minimum requirements and activities for the purchase of IT goods and services to ensure the IT security and data risks are assessed prior to APS data being put at risk. Requirements in these policies or regulations should be part of the District procurement process and enforceable for all IT goods and services.

Rausch recommends APS:

- ✓ Define minimum-security requirements for technologies including software and SaaS or cloud solutions
 - Checklists or standards for each anticipated solution type should be developed to assist District personnel when identifying technology solutions. Questionnaires with decision trees to help identify the appropriate controls should be considered.
 - Specific minimums should be considered over general requirements. For example, state the minimum encryption strength required rather than stating that data must be encrypted.
- ✓ Consider IT security and data risks when determining the required approval and review activities. Current processes focus on the dollar amount of the purchase to identify required activities. The purchase amount, however, is not appropriate to determine the presence of IT Security or Data risks. Many software solutions or “Apps” have minimal costs. The specific use and the implementation methods should also be evaluated to determine the appropriate level of assessment activities needed.
- ✓ Require a security risk assessment for all IT purchases prior to the contract being signed or the purchase executed (as in the case of P-Card purchases). Assessment activities should be commensurate with the risks presented by the technology being considered. For example, short

questionnaire may be sufficient for an off-the-shelf solution, but a more detailed assessment would be required for cloud solutions to process or store student or employee data.

- ✓ Work with IT Security to define circumstances which should require IT Security review and define as requirements within the procurement process.
- ✓ Add an IT Security approval on the solicitation agreement to reflect the completion of the security risk assessment activities. Separation of IT and IT Security approvals would help ensure the solution is evaluated for both the technology compatibility and the security requirements.

Management's Response

Management agrees with this finding. The IT Department has created a Third-Party Oversight Standard that defines the security requirements for IT purchases. The IT, Procurement and the Governance & Policy departments are working together to create a district regulation. This regulation is in draft form CNA (R2).

Management's Implementation Plan

1. Update Regulation to reflect security requirements defined in 3rd Party Oversight Standard
2. Create Security Assessment for purchasing of IT services, hardware, and software.
3. Perform security assessments for existing vendors.

Anticipated Completion Date

December 31, 2020

Responsible Party

Carrie Roberts, Executive Director, Purchasing
Roanna Washington, Director IT Security & Network Services

2. Contract Language Does Not Contain Specific Language to Address IT Security and Data Risks

Finding

Specific requirements to address IT security and data risks to protect APS data are not defined in contracts. Vague language is used that does not specify the level of protection or minimum requirements. For example, the Blackboard 2013 agreement, Section 6.2 states, "Contractor shall take all commercially reasonable measures necessary to keep the Confidential Information confidential, including, without limitation, all measures it takes to protect its confidential information of a similar nature." Commercially reasonable measures vary from password protection to encryption. Without specific language, the vendor may comply with the contract yet still not apply the level of protection needed to protect APS.

Key items not found in the contracts reviewed include:

- Activities requiring the vendor to monitor their own IT security and data risks
- Roles and responsibilities were not always fully addressed nor did the contract require these to be documented
- Provisions to give APS the authority to conduct security assessments of the vendors security controls and processes

Additionally, Rausch noted contracts signed more than five years ago continue to govern the use of the implemented technologies. Relevant privacy and security terms are not included. In one instance the security framework referenced by the vendor is obsolete. The contract references adherence to NIST Special Publication 800-26, however, that standard publication was superseded in 2007 yet it remains included in 2015 and 2016 agreements. This standard does not address current technologies such as cloud services and may not address all current security risks.

The privacy and security landscape and technologies are continually changing. Decisions made as little as five years ago may no longer provide the security or up-to-date data protection features best solution or option for APS. Furthermore, processes to involve IT and IT Security in the renewal decision were not identified.

Risk

APS data may not be protected from unauthorized access or loss when collected, stored, or processed by third-party solutions or services.

APS may not have recourse to address losses if contracts do not include privacy or security requirements to comply with current security and technology risks.

Vendors may not maintain current or compliance with new technology standards or regulations.

Recommendation

NIST CSF Control: ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.

NIGP The Institute for Public Procurement, Principles and Practices of Public Procurement, Element 1: Procurement should use solicitation templates specifically developed for the procurement of IT software. These templates must safeguard the ownership and security of data, records, and other procurement-related information from contract award through contract completion, while guiding the parties to a mutually acceptable contract.

APS should require vendors provide the same or greater security and data protection levels as if APS were performing the service or supporting the product internally. These requirements should be defined in

contracts to protect APS and provide legal recourse. Rausch recommends contract language address key activities necessary to protect systems and data including (but not limited to):

- ✓ Right to audit clauses to allow APS the ability to assess the security posture of the vendor.
- ✓ Requiring the vendor have independent assessments of their security controls and processes.
- ✓ Specification of the location of APS stored data (i.e., remaining within the US), the origin of data entering the vendor's system, and any restrictions concerning data access and overall data security (i.e., encryption).
- ✓ Specifying the minimum encryption levels for data at rest and in-transit
- ✓ Specifying equipment disposal requirements and standards to protect against data loss.
- ✓ Specifying how security breaches or incidents will be handled and reported.
- ✓ Specifying responsibility for securing supplier systems stored at the entity's site.
- ✓ Specifying the steps necessary to ensure supplier compliance with policies, laws, and regulations concerning data security, e.g., security practices questionnaire.
- ✓ Specifying data triage procedures in the event problems are encountered.
- ✓ Roles and Responsibilities should be clearly documented. Activities such as day-to-day support, backup responsibilities, and incident response should be clearly defined to ensure all activities are addressed.

Processes to renew contracts should consider technology changes, new security threats, and new or pending privacy regulations. Contract language should be reviewed when contracts are renewed to ensure current security risks are addressed. IT Security should be included in the contract review process, where appropriate, to ensure technology clauses address current IT security and data risks and applicable laws.

Management's Response

Management partially agrees with this finding. Standard security terms and conditions are defined in the APS contract. However, specific/detailed security requirements are typically addressed in the Statement of Work (SOW) for each project. We will work jointly with Legal to review standard security terms and conditions in the contract.

Management's Implementation Plan

We will work jointly with Legal to review standard security terms and conditions in the contract and on purchase orders.

Anticipated Completion Date

July 31, 2020

Responsible Party

Olufemi Aina, Executive Director, Information Technology
Roanna Washington, IT Security & Network Services
Carrie Roberts, Executive Director, Purchasing

3. A Process for Monitoring Third Parties for IT Security and Data Risks is Not Implemented

Finding

APS does not perform activities to monitor third parties to ensure IT security and data risks are addressed. Discussions with Procurement, IT Security, and key business users, revealed only one instance where an independent assessment report (SOC2 for Infinite Campus) was collected from the vendor; however, evidence regarding its review was not documented nor were standards identified to guide the review activity.

Risk

APS data may not be protected from unauthorized access or loss when collected, stored, or processed by third-party solutions or services.

Recommendation

NIST CSF Control: ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.

Security Assessments should be performed throughout the life of the contract at a frequency commensurate with the associated risk to ensure vendors/third parties demonstrate they are compliant with contract requirements and/or APS security practices. Minimum requirements for the reviews should be established and the reviews should be performed by the IT Security Department or qualified third party.

Reviews should be documented, and results shared with the APS business owner or relationship manager. Issues noted should be tracked through resolution. Contract review activity should consider assessment results and the status of identified issues.

Examples of review activities may include gathering responses and documentation by administering a security questionnaire, reviewing the results of an independent assessments such as SOC2, or performing an IT Security audit of the vendors security controls and processes.

Management's Response

Management agrees with finding.

Management's Implementation Plan

IT will work jointly with the Purchasing to create a process to review IT security risks for 3rd party vendors.

Anticipated Completion Date

December 2020

Responsible Party

Olufemi Aina, Executive Director, Information Technology

Roanna Washington, IT Security & Network Services

Carrie Roberts, Executive Director, Purchasing

4. Current Processes Do Not Provide District-Wide Visibility or Oversight of IT Vendors

Finding

District Purchasing nor IT Security have visibility to all IT purchases. Schools have autonomy to make purchases, including technology, which may or may not involve Procurement or IT prior to the purchase. Additionally, Rausch learned IT products and services may be purchased using purchasing cards (P-cards). In these cases, the vendor may not be reviewed by IT prior to purchase.

Furthermore, vendors are not identified or categorized in relation to their IT security and data risk within the District's primary vendor management system, Lawson nor in the school financial system, SABO. All IT vendors or vendors that store, process, or access APS data throughout the District cannot be identified.

To identify IT vendors, Rausch reviewed the Lawson Vendor Master List, a vendor listing from SABO (school financial system), and an Enterprise Application list maintained by IT. Rausch noted that in Lawson, the vendors are not identified (categorized) in relation to their IT security and data risk. An Enterprise Application list provided by IT (actual systems in use) was then used to select vendors from the Lawson or SABO listings. Vendors on the Enterprise Application list provided by IT (actual systems in use) were not found on either the Lawson or SABO listings.

In two instances contracts for vendors used by schools could not be located. Contracts for Educator's Handbook (a cloud solution used to document and troubleshoot office referrals and minor incidents at the district, school, grade, employee, and student levels) and ScholarChip Visitor Management (a web-based system that automates visitor data collection, secures entries and maintains historical data on all incoming campus visitors across a school building or district) are not maintained by the District's Procurement department. Educator's Handbook was included in the Lawson Vendor Master file; however, ScholarChip Visitor Management was not found in Lawson or SABO (school financial system) nor the Lawson system.

Risk

Technology services, including software and cloud service providers (Software-as-a-Service), may be purchased without assessing IT Security or data risks nor IT compatibility.

Recommendation

NIST CSF Control: ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process

Rausch recommends technology purchases regardless of the payment source, should require IT Security review prior to being purchased. Minimum requirements for all technology products should be identified in District-wide procedures.

To facilitate risk and monitoring activities, vendors that store, process, or access APS data or information systems should be easily identified within purchasing or accounting systems.

Management's Response

Management partially agrees with this finding.

- IT Department purchases and vendors - all technology and vendors go through the procurement process. For schools that purchase technology items using the approved vendors, the procurement process works.
- With flexibility and autonomy given to schools, they have the ability buy different instructional software that may not always go through the IT purchasing process. The IT and Purchasing departments are working together to rein in on those purchases. All other avenues to purchase technology using unauthorized vendors have been blocked.

Management's Implementation Plan

1. Complete software purchasing process.
2. Management is working on solutions within the Lawson system to incorporate the use of NIGP codes to categorize vendors and track purchases. The implementation of these codes into the current vendor databank would require an increase in staffing resources, as there are over 85,000 vendors in the current vendor database and all vendor records would require review and update.

Anticipated Completion Date

1. August 2020
2. December 2021

Responsible Party

Carrie Roberts, Executive Director, Purchasing