SaaS - Data Sharing and Transfer

Internal Audit Report

January 31, 2022

Orange County Public Schools
Internal Audit

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

Table of Contents

EXECUTIVE SUMMARY

Why We Did This Audit

The objective of this audit was to determine whether the district is performing data transfers in a secure manner by analyzing the means by which the data is shared with vendors and other third parties.

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
<u>Source</u> IA - Internal Audit or M - Management	IA - 1	IA - 1	IA - 1
<u>Observation Category</u> D - Deficiency or O - Opportunity	D - 1	O - 1	D - 1

Our overall conclusion is that the District is generally performing data transfers in a secure manner. The following measures are in place:

- Approved policies, procedures and most applications met the District's minimum acquisition requirements
- Most vendors are vetted
- The district has gathered key details about most SaaS applications such as SOC reports, system documentation, types of shared data, means of transfer, responsibility for the transfer, whether other -parties are involved and the type of cloud environment that the data is in. However, the importance of these details in some cases was not understood by the personnel.
- The SaaS definition is aligned to a reliable technology source
- A reliable technology framework is used for implementing oversight measures for access controls

Results and Recommendations

We evaluated control procedures and performed various tests to determine whether they are effective. We noted important documentation of SaaS vendor controls was missing, one SaaS vendor has no contractual relationship with the district, data transfers with two SaaS vendors are not conducted via secure methods and an important ITS standard dealing with third-party information security has been developed but not implemented.

Based on the results of our audit, we made three recommendations:

- Have a direct contractual relationship with vendors with access to district data.
- Use a checklist to document important steps that are being missed on the vendor's due diligence before entering in a contractual agreement.
- Make ITS standard InfoSec 006, Third-Party Information Security, readily available to the District personnel so they will know in advance District policies.

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 the observations resulting from this audit were sourced to management.

BACKGROUND:

Software-as-a-Service (SaaS) is a software licensing model in which access to the software is provided on a subscription basis, with the software being located on external servers owned by others rather than on district servers located in-house. SaaS is typically accessed through a web browser, with users logging into the system with a username and password. Instead of each user having to install the software on their computer, they are able to access the program via the Internet.

These district departments manage and/or use SaaS applications:

ITS Business Applications Group

The Applications area is responsible for school and business software application development for the district. They provide design, development, implementation, and support services needed for integration of enterprise solutions and automation of the District's business processes.

SIS & Projects Department

The Student Information Systems (SIS) department provides configuration, maintenance, support, and training for the administrative student information system – Skyward. It also provides student source data to approximately 100 other systems.

Human Resources Department

The Human Resource Department uses the SaaS application iCIMS as their applicant tracking system.

Payroll Department

The Payroll Department uses the SaaS application Kronos to register time attendance and absences for most employees paid by the hour.

Teaching & Learning

The Teaching & Learning Department uses a SaaS application called ClassLink. This application shares and transfers data to 71 other applications[1].

SaaS applications are used by:

- *ITS Business Applications Group*
- *SIS & Projects*
- *Human Resources*
- *Payroll*
- *Teaching & Learning*

[1] According to a data sharing report prepared by the Senior Director of Curriculum & Digital Learning dated 10/12/2021.

OBJECTIVE, SCOPE AND METHODOLOGY:

Objective

The objective of this audit was to determine whether the District is performing data transfers in a secure manner by analyzing the means by which the data is shared with vendors and other third parties.

Scope

The scope of the audit was FY 2020-21 and current data transfers.

Our scope included current data transfers and from Fiscal Year 2020-21

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. We noted no material deficiencies in this audit. We also offer suggestions to improve controls or operational efficiency and effectiveness.

We noted no material deficiencies in this audit.

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

Our audit steps included specific audit procedures to determine what controls exist and their effectiveness.

- Interviewed personnel from the ITS, SIS & Projects, HR, Payroll, Teaching and Learning and Finance Departments and contractors (when applicable)

- Compiled a list of SaaS applications that share or transfer data and evaluated whether acquisition requirements were met and required documentation had been obtained.

We compiled a list of SaaS applications.

We tested controls and procedures.

- Tested controls and procedures related to established methodologies and practices for SaaS applications and reviewed the following:
    - District policies and procedures for SaaS applications and data transfers
    - The district's definition of SaaS and their purpose
    - Security measures in place to monitor different activities within these applications
- Evaluated data transfer protocols for data at rest, in-motion and in-use states

RESULTS & RECOMMENDATIONS:

Overall Conclusion:

Our overall conclusion is that the District is generally performing data transfers in a secure manner. The following measures are in place:

Our overall conclusion is that the District is generally performing data transfers in a secure manner.

- Approved policies[2], procedures and most applications met the District's minimum acquisition requirements
- Most vendors are vetted
- The district has gathered key details about most SaaS applications such as SOC reports, system documentation, types of shared data, means of transfer, responsibility for the transfer, whether other - parties are involved and the type of cloud environment that the data is in. However, the importance[3] of these details in some cases was not understood by the personnel.
- The SaaS definition is aligned to a reliable technology source
- A reliable technology framework is used for implementing oversight measures for access controls

Although key details are generally obtained for SaaS applications, staff do not always understand their significance.

We noted an opportunity to improve the district's collection of key details from SaaS vendors. We also noted two deficiencies – one where

[2] Including an acquisition policy.

[3] The "why we should need this information."

the district has no direct contractual agreement with a vendor that uses our data in providing services and one where the policy establishing security requirements applicable to third-parties that handle confidential information has not been shared or published to the personnel who would implement it. Our detailed findings and recommendations follow.

We noted one opportunity and two deficiencies.

1) Vendors with access to district data should have a direct contractual relationship with the district ***Significant Risk or Impact***

Best Practice:

Contracts are a vital part of building relationships and completing business transactions. Contracts are important for reasons that include:

- They serve as a record of commitments for both parties - At their very core, contracts are the basis for relationships. A contract is the visual representation of that relationship. Contracts also hold each party to their original agreement.

- Agreements prevent conflicts and mitigate risk - Contracts often go through a negotiation process that ensures both sides are getting the best deal possible and that both parties interested are protected. Good contracts should lead to a mutually successful outcome and prevent conflicts down the line.

Contracts serve as a record of commitments for both parties and help to prevent conflicts and mitigate risks.

Audit Result:

Teaching & Learning uses an application called ClassLink for a number of critical functions: LaunchPad, Roster Server and ClassLink Analytics+. This application makes extensive use of district and student data. ClassLink was acquired through a third-party vendor named CDW. The district has no contractual relationship with ClassLink.

We acquired a key SaaS application through a third-party vendor.

This means none of the district's standard data protection and security clauses govern this relationship. Should ClassLink experience a data breach or have other issues with our data, we would have no contractual recourse against them.

If the SaaS application vendor mishandles our data, we have no contractual recourse against them.

There may be other applications acquired through similar means that were not part of our audit scope.

Recommendation:

Have a direct agreement[4] signed with any vendor providing the district with a service, especially those involving our data, in order to have accountability for both parties in case something happens. The district should search for other arrangements where such an agreement may be necessary.

Have a direct agreement with any vendor providing services that use our data.

2) Use a checklist to insure important steps are not missed in the due diligence process before entering a contract.

Moderate Risk or Impact

Best Practice:

To mitigate risks associated with third-parties having access to district data, vendors should be vetted and certain information should be obtained and evaluated prior to entering into a contractual relationship. Some of the more important information includes:

Engaging with SaaS vendors requires due diligence prior to entering a contract.

- **Functional Requirements or Technical Specifications** - Define the basic system functionality: what it can and can't do. It also includes information about the owner of the functionality [who requested it], designer, developer, quality assurance [UAT[5]], and the technical requirements.

- **System Documentation** - System documentation describes the system itself and its parts. It usually consists of the requirements document, architecture design, source code, validation documents, verification and testing info, and a maintenance or help guide.

- **Backups** - information about data backups assures that data restoration will occur in a timely manner according to the district's needs in the event of a data loss.

With cloud computing technologies, vendors offer different kinds of services over the web or similar networks. After the above information has been evaluated and is satisfactory to the district, the next steps involve obtaining and evaluating:

Certain factors should be evaluated before engaging the SaaS vendor:

- **Data share agreement with all non-vendor third-parties** - this is a formal acknowledgement of any non-vendor third parties who

❖ *Who has our data?*

[4] It could be a contract, a data share agreement or any other type.

[5] User Acceptance Testing.

have access to our data either by a mutual vendor or by a vendor of a vendor [4th-party]. This can help the district understand its exposure and establish responsibility in case of a breach.

- **Where the solution is located** – the district's standard contract language indicates our data should remain within the states, districts, and territories of the United States unless specifically agreed to in writing by an SBOC officer with designated authority. This helps to avoid international litigation processes in foreign countries where laws can differ and are not subject to US jurisdiction.

- **Hosting agreement between vendor and the hosting facility** - so the District knows what to expect from the hosting facility in terms of SLA's[6], location and availability among many others.

- **Hosting facility [vendor or other third-party] business continuity & disaster recovery plan** – where SLAs are not established, the district needs to know whether the vendor has a business continuity & disaster recovery plan and whether that plan meets district's needs.

The following documentation would provide most of the information described above about a vendor's environment. During our audit, we expected the district to have this information in some form:

- **SOC 2 Reports** – these audit reports address five trust service areas: security, availability, processing integrity, confidentiality and privacy. They are the gold standard for assurances about vendor control effectiveness.

- **Who's responsible for the transfer** - sometimes, a group or an employee may be responsible for creating the script that will produce the transfer to send the data to the vendor's environment.

- **Other third-parties involved apart from the vendor** – a vendor may rely on other vendors to accomplish their work for the district. *Vendor A* may have a contract with *Vendor X* to store the district's data in their cloud environment. Unless this arrangement is disclosed, the district may believe its data is at *Vendor's A* environment.

❖ *Where are our data?*

❖ *What will the various parties do with our data?*

❖ *Do parties other than our vendors have access to our data?*

SOC 2 audits are the gold standard for assurances.

Know who is responsible for each phase of the data transfer.

Know what other parties have access to our data and evaluate their control processes.

[6] Service Level Agreements

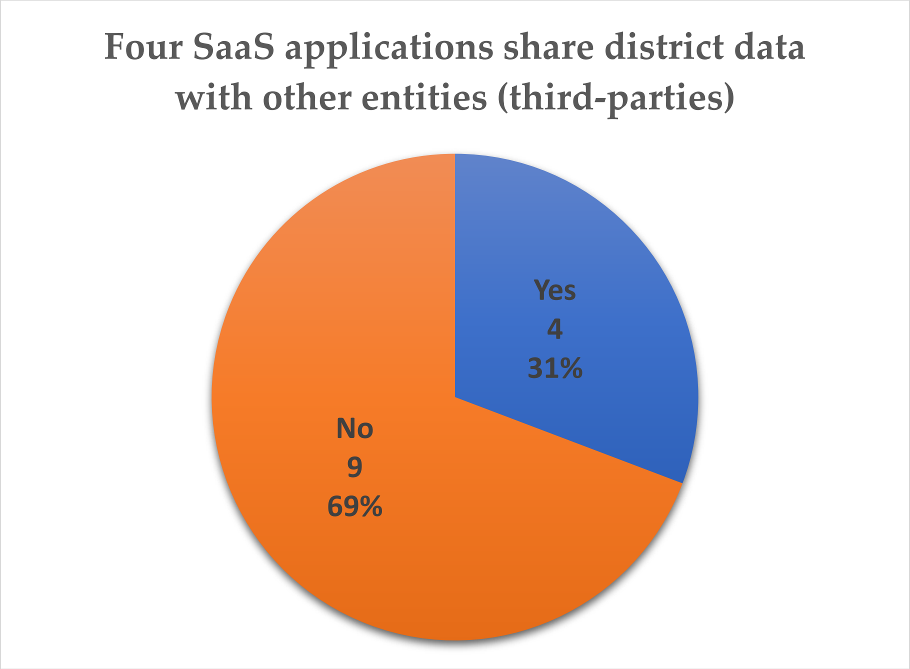
Audit Result:

We evaluated 13 SaaS applications[7] used by the district that transfer or share data and determined whether:

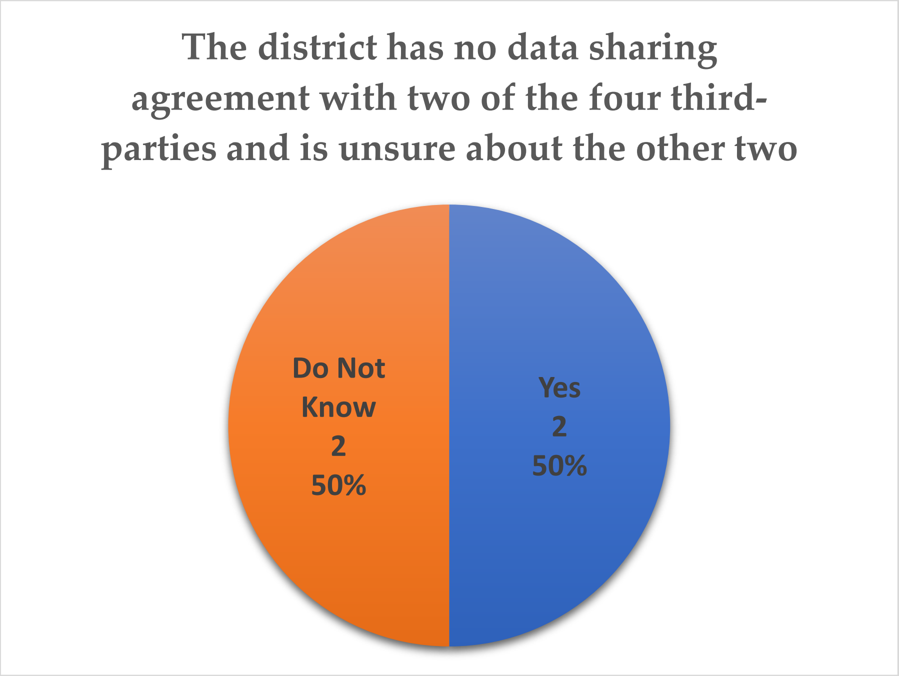
- They met the requirements of the original solicitations;
- The district had obtained and evaluated key details about the vendors such as whether the data being shared with the vendor is shared by the vendor with another third-party; whether the application is hosted by another third-party instead of the vendor; what type of cloud environment the data is in; where the application or system is hosted; whether the hosting facility has a business continuity & disaster recovery plan; and
- The district had obtained documentation such as SOC 2 Reports, system documentation, type of data transfer, and type of cloud environment, among many others.

We have depicted the results of this testing in the following charts.

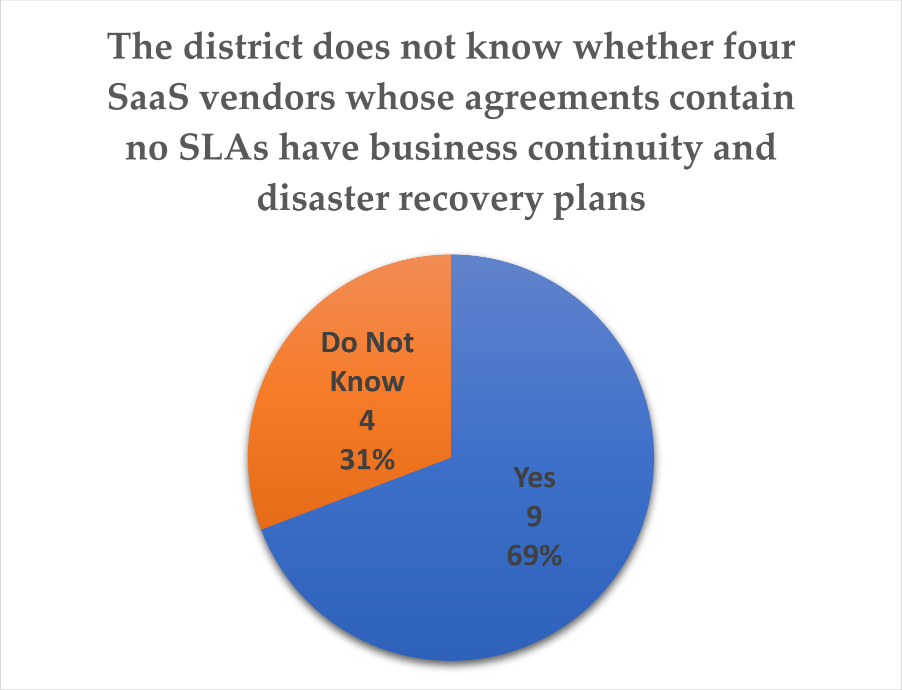
Four of the 13 SaaS applications evaluated share district data with other parties.



[7] Skyward; iCIMS; Kronos; School Funds Online; School Pay; ClassLink; i-Ready; ExploreLearning Gizmos; Microsoft SDS; Springboard; Canvas; Performance Matters; and Test Hound.



The district has no data sharing agreement with two of the four third-parties and is unsure about the other two

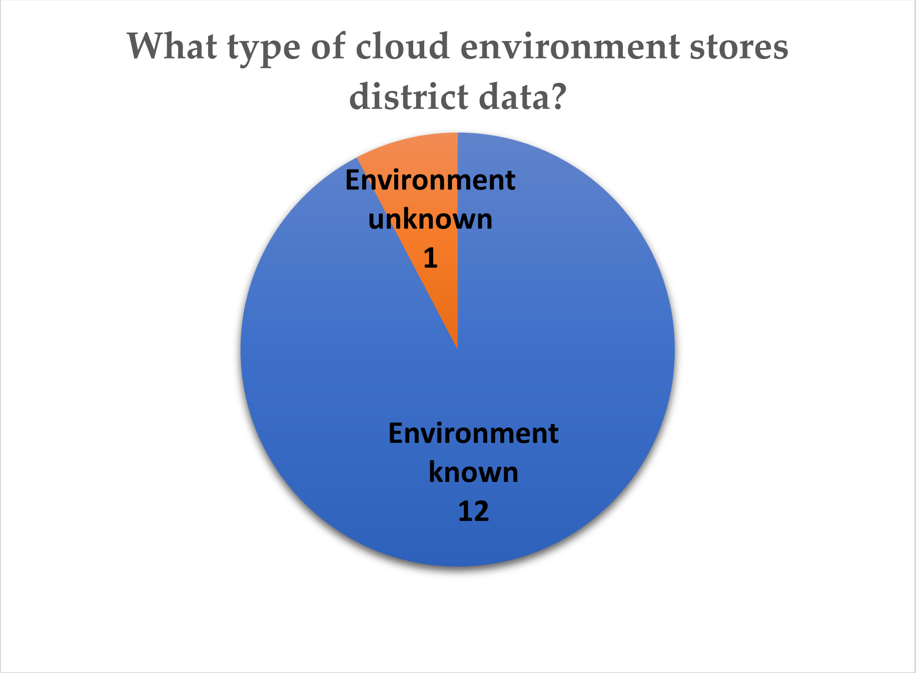


The district does not know whether four SaaS vendors whose agreements contain no SLAs have business continuity and disaster recovery plans

The district does not know where the data is for two of the third parties and has no data-sharing agreement with the two that are known.

The district does not know whether business continuity and disaster recovery plans exist for four of the 13 SaaS applications. Also, these four applications have no SLAs in their agreements with the district.

Eleven of the 13 SaaS applications we reviewed are hosted by a party outside the agreement between the vendor and the district. Additionally, the district knows the type of environment (public, private or hybrid) where its data is stored for 12 of the 13 SaaS applications. See the chart below:



Out of 13 tested SaaS applications, we noted the following:

Information that should be obtained in the due diligence	Obtained	Not obtained
SOC 2 Report	7	6
System Documentation	7	6
Type of shared data	11	2
Means of transfer	11	2
Transfer responsibility	10	3
Other 3rd Parties	6	7
Type of cloud environment	12	1

Eleven of the 13 SaaS applications are hosted by a party outside the agreement between vendor and district.

The district has no knowledge of the environment where its data is stored for one application.

Key documentation had not been obtained and evaluated for SaaS applications.

Recommendation:

We recommend personnel in charge of selecting the vendors for any SaaS solution develop and use a checklist that has all the documentation that is needed prior to formalizing an agreement. This will help to ensure no critical information is overlooked and help make an informed decision based on the information evaluated.

Use of a checklist may help to ensure important documentation is obtained and evaluated.

3) ITS Department standard InfoSec 006, Third-Party Information Security, has not been published or shared to District personnel. ***Minor Risk or Impact***

Best Practice:

Important organizational policies that can affect the daily tasks of any organization need to be shared with those who should implement them.

It is important to share organizational policies that can have an effect on the daily tasks of any organization.

Audit Result:

InfoSec 006 is part of the district's Software Approval Application Process and establishes "*security requirements for the use of third parties that handle OCPS confidential information, either by storing, processing, transmitting or receiving information.*" This standard describes controls to reduce the information security risks associated with contracted services and staff and includes specific procedures that are to be followed to accomplish this.

This standard describes controls to reduce risks associated with third-parties that handle district data and establishes specific procedures that are to be followed.

These controls are mapped to NIST Special Publication 800-53 R4[8], CIS[9] 20 and Cyber Security Framework. We evaluated this Standard and found it to be effective, if followed, in reducing risks to the district. However, it has not been implemented.

Regarding InfoSec 006, the ITS department noted that it is to be reviewed with the Procurement department as part of the Third - Party audit. Regarding future state of this standard, ITS is planning to post it on the department’s intranet page.

Standards cannot be followed if they are not known to those who would implement them.

[8] Security and Privacy Controls for Information Systems and Organizations.

[9] Center for Internet Security.

Recommendation:

We believe the procedures described in this ITS Standard are important to effective management of risks associated with third-party relationships and they should be implemented as soon as practicable. We recommend this standard be widely communicated to district personnel so they will know the district's requirements. We also recommend a training plan be developed to ensure effective implementation.

This is an effective standard and it should be implemented.

We wish to thank the personnel from the ITS, SIS & Projects, Payroll, Finance Departments and Teaching & Learning (including contractors) for the cooperation and assistance we received in the course of this audit.

AUDIT RESPONSE MATRIX: SOFTWARE AS A SERVICE DATA SHARING & TRANSFER
FISCAL PERIOD OR AUDIT DATE: JANUARY 31, 2022

Department / School Name	**ITS & Procurement**
Administrator / Department Head	**Russell Holmes & David Wheeler**
Cabinet Official / Area Superintendent	**Robert Curran & Roberto Pacheco**

Audit Result / Recommendation	Management Response Acknowledgement/ Agreement of Condition	Responsible Person (Name & Title) And Target Completion Date	Management's Action Plan
Vendors with access to district data should have a direct contractual relationship with the district/ Have a direct agreement signed with any vendor providing the district with a service, especially those involving our data, in order to have accountability for both parties in case something happens.	Management acknowledges/agrees with this audit result and recommendation	David Wheeler Director Procurement Russell Holmes Sr. Director ITS 07/2022	The district will work with procurement and ClassLink to develop a direct agreement signed by the vendor at the upcoming renewal period. Staff will also review purchases made through third party resellers to determine if the software purchased collects data, in which case an agreement may be implemented.
Use a checklist to insure important steps are not missed in the due diligence process before entering a contract.	Management acknowledges this audit result and recommendation	David Wheeler Director Procurement Ongoing	Contracting terms and conditions as well as processes are continually evolving and improving. Procurement Services utilizes a process checklist for all contracts to ensure the most current agreement templates are utilized when entering into a new contract with a vendor.
ITS Department standard InfoSec 006, Third-Party Information Security, has not been published or shared to District personnel.	Management acknowledges and agrees with this finding.	Russell Holmes 05/2023	A link to the Department standard InfoSec 006, Third-Party Information Security has been posted on the ITS Information Security Policies & Guidelines Intranet page. As this applies to those completing a software approval request, an update is being proposed to add a link referencing the

			Infosec 006 standard. Additionally, a required check box will need to be marked, before submission of the form, indicating that the standard has been read. These proposed changes to the Software Approval Process are currently pending committee approval.