Skyward Interfaces Audit

Access & Security (Logical & Physical)

Internal Audit Report

August 4, 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 overall objective of this audit was to evaluate the effectiveness of the district's security for Skyward interfaces. To accomplish this, we divided this audit into three phases:

- Policies and procedures
- Access & security (logical and physical)
- Types, completeness, accuracy and control of interfaces

In this phase, the objective was to determine whether effective logical & physical access and security were documented and implemented for the Skyward system, folders and/or modules where critical data is located that are used by the SIS & Projects department.

This audit was included in the 2020-2021 Annual Audit Plan.

Observations and Conclusion

Our overall conclusion is that the SIS & Projects department has documented and implemented effective logical and physical accesses security for the Skyward system, its folder and modules where the critical data is located. They have documented physical and logical security measures for the hardware that houses the critical data for Skyward operating effectively.

Results and Recommendations

We evaluated the access and security for both physical and logical points of entry of the Skyward system and based on the results, we recommend that they perform due diligence in the form of a checklist or by other means to obtain and evaluate information needed from prospective vendors such as location of the system, who's hosting it, type of cloud, and business continuity and disaster recovery plans, among many others, before entering in a contractual agreement.

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

BACKGROUND:

This audit report is part of an overall review of the Skyward system interfaces. Skyward is the district's student information system. This Software-as-a-Service product provides the district with various functionalities such as student management, state reporting and gradebook among many others.

This interface audit is being conducted in three phases: Policies and Procedures; Access & Security (Logical and Physical) and Types, Completeness, Accuracy & Control of Interfaces. This report is for the Access & Security (Logical and Physical) phase. Previously, we issued the Policies and Procedures report. The Types, Completeness, Accuracy & Control of Interfaces audit is paused until the Student Information Services Department completes a number of priority projects that make their participation in an audit impracticable at present.

As of December 8th, 2021, the Skyward system had a total of 103 interfaces (12 with internally-hosted systems and 91 with externally-hosted systems, 60 of which are for class courses). The majority of these interfaces are exports from the Skyward system, but the list includes imports, exports and imports/exports.

Webopedia defines interface as a boundary across which two independent systems meet and act on or communicate with each other. In computer technology, there are several types of interfaces. They mention three types of interfaces: user, software and hardware:

- User interface - the keyboard, mouse, menus of a computer system. The user interface allows the user to communicate with the operating system.
- Software interface - the languages and codes that the applications use to communicate with each other and with the hardware.
- Hardware interface - the wires, plugs and sockets that hardware devices use to communicate with each other.

So, an interface can occur at the logical (software), physical (hardware) and user levels. This phase focused on the logical and physical aspects of the interface.

When referring to software, an interface is a program that allows a user to interact computers in person or over a network.

An interface can also be defined as a tool and concept that refers to a point of interaction between components, and is applicable at the level of both hardware and software.

Another definition for interface is a boundary across which two independent systems meet and act on or communicate with each other. In computer technology, there are several types of interfaces.

OBJECTIVE, SCOPE AND METHODOLOGY:

Objective

The overall objective was to evaluate the effectiveness of the District's security for Skyward interfaces. In this phase, the objective is to determine whether effective logical & physical access and security were documented and implemented for the Skyward system, its folders and/or modules where critical data is located.

The objective in this phase was to determine whether effective logical & physical access and security were documented and implemented.

Scope

The scope of the audit assessed interfaces based on criticality and importance to the Skyward system and to district operations. In this phase, we focused on the Skyward folders and/or modules where critical data is located and are used by the SIS & Projects department[1].

We assessed the interfaces based on criticality and importance to the Skyward system.

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 in this audit.

Our tests measured and determined whether logical and physical access and security were in place for the Skyward system, folders and/or modules.

[1] This 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.

For this, we assessed access and security by evaluating:

Access and Security (Logical and Physical)

- Logical Access
  - Software - which software is interacting with Skyward thru an interface (SaaS and non-SaaS)?
  - Users - who has access to perform these interfaces (possible third-party user access)?
  - Networks - who has access to it (possible third-party user access)?
  - Folders or databases - who has access to the Skyward data that is being transmitted through the interfaces and where the data resides? Skyward data resides on two points: in the main database and in the replication database. Both are located in Wisconsin. According to the interfaces data flow map, the replication database sends data to the Enterprise Data Warehouse (EDW), which is located in Florida.
- Physical Access
  - Hardware - which devices are interacting where the Skyward data resides?
  - Server Rooms - who has access to physically enter the environment (the data is in Wisconsin[2] and in Florida[3])?
- Logical Security
  - What security measures are in place to control all logical access points to where the Skyward data is and goes[4] (passwords for user logins and network access, access only to certain folders, only by certain employees, etc.)?
- Physical Security
  - What security measures are in place to control all physical access points, if available and known to the district (key cards, access lists for server rooms, allow access to certain devices or hardware only, computers, etc.)?

Our tests included logical and physical access and security review for the following:

- *Software*
- *Users*
- *Networks*
- *Hardware*
- *Server Rooms*
- *Access Points*

[2] It is a good practice to know who can access the physical environment in Wisconsin
[3] Thru EDW
[4] If available and known to the district

RESULTS & RECOMMENDATIONS:

The district has effective logical and physical accesses, both documented and implemented, for the Skyward system, but we found an opportunity within the documentation of externally hosted systems.

Overall Conclusion: Our overall conclusion is that the SIS & Projects department has documented and implemented effective logical and physical accesses for the Skyward system, its folders and modules where critical data is located. Also, they have documented effective physical security measures[5] for the hardware that houses critical data for Skyward.

As for the logical security of the Skyward system, its folders and modules where the critical data is located, they have documented measures and in place, operating effectively. However, we did find an area of opportunity within the documentation of externally hosted systems.

Our detailed findings and recommendations follow.

1) Perform due diligence in the form of a checklist to document important information from the vendor before entering in a contractual agreement. ***Moderate (Risk or Impact)***

Best Practice:
Relationships with third parties are among the most significant risk to an organization's information systems. It's a best practice for any organization to evaluate risks associated with third parties by performing due diligence procedures before entering these relationships. Due diligence procedures include obtaining documentation such as continuity plans, location of systems and list of third-parties, among many other things, from vendors that want to obtain a contract with the organization. This, in order to better understand the vendor's environment and how they are going to help an organization achieve its goals without compromising its data. Examples of the types of documentation that should be reviewed are below:

[5] For this, we reviewed the most current SOC 2 Type 2 report of the facilities where the hardware and equipment are located.

- Business Continuity & Disaster Recovery Plans (**vendors**) – this is to see whether the vendors have any type of business continuity plan for disasters or any disruptive events that might interrupt their services, which in turn might affect the district's day-to-day operations, and how they're going to restore operations.

- Type of cloud environment - when it comes to migrating traditional local software applications to a cloud-based platform, data security may be a problem. When a computer and application is compromised the SaaS multi-tenant application supporting many customers could be exposed to the hackers. Any provider will promise that it will do the best in order for the data to be secure in any circumstances. But just to make sure, the district should ask about the provider's infrastructure and application security.

- Where the systems are hosted - data should always remain in the US, whether is in the continental US[6] or any of the US territories[7]. This could be mainly to avoid any international litigation processes in a foreign country. In other words, the district has to be aware where its data is located. Although the Federal Information Security Management Act requires customers to keep sensitive data within the country, on virtualized systems the data can move dynamically from one country to another. Ask about the laws for your customers data in respect to where they are located.

- Business Continuity and Disaster Recovery plans (vendor's third parties) - sometimes, a vendor may rely on their own vendors for their business to be productive. This could mean that vendor A may have a contract with vendor X to have the district's data in their cloud environment and for the District eyes it will look like their data is at vendor's A environment. That's why is extremely important for the district to inquire about any documentation that the third-parties from their vendors may have, in this case, the BC & DR plans.

Audit Result:

Based on our audit procedures, we concluded the interfaces are partially documented. Detailed results, based on evidence received from district BPOs and vendors, are in the following table:

For some interfaces that go into the Skyward system, the district was not aware of the following aspects, among many others:

- *Where the systems are hosted*
- *Who's hosting the system*
- *Type of cloud environment*
- *If the vendor has a Business Continuity (BC) and Disaster Recovery (DR) plans*
- *Whether there is an agreement between the district's vendor and their hosting facility (vendor's third-party)*

[6] This includes the 49 states located on the continent of North America and the District of Columbia

[7] Puerto Rico, the U.S. Virgin Islands, Guam, Northern Mariana Islands and American Samoa

Information that should be obtained and documented[8]	Obtained	Not obtained	N/A and/or INP[9]
Signed Agreement	11	0	0
Where the systems are hosted	6	1	4
Who's hosting the system	7	1	3
Type of cloud environment	5	3	3[10]
If the **vendor** has BC and DR plans	7	1	3
If the district has a copy of the **vendor's** BC & DR plans	1	6	4
Who's hosting the environment (Vendor, Third-Party or Cloud)	8	3	0
If there is an agreement between the district's **vendor** and their hosting facility (vendor's third-party)	2	0	9
Knowledge that this facility (**vendor's third-party**) has BC & DR plans	2	0	9
If the district has a copy or access to the **vendor's third-party** facility's BC & DR plans	2	0	9
When the data is at rest outside the district's environment, knowledge of what measures are in place to determine that the data is complete and how they (**vendor** or **third-party**) prevent any changes to it	2	0	9

[8] From the total of system interfaces analyzed (12), one system was a purchased software and it will not be considered in the totals. The columns (Obtained, Not Obtained and N/A and/or INP) should totaled 11.
[9] Information Not Provided.
[10] These were on-premises software (non-cloud).

Recommendation:

We recommend personnel in charge of selecting the vendors for any future interface with the Skyward system perform a due diligence in the form of a checklist or by other means to verify the information needed from a prospective vendor is obtained and evaluated before entering in a contractual agreement. This will help to ensure no critical information regarding the interfaces is overlooked and help make an informed decision based on the information evaluated.

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

The district should perform due diligence with prospective vendors by obtaining and reviewing the following system information, among many, in order to make an informed decision:

- *Location of the system*
- *Who's hosting it*
- *Type of cloud*
- *Business Continuity and Disaster Recovery plans*

Department / School Name	**Student Information Systems & Projects**
Administrator / Department Head	**John A Davis – Executive Director**
Cabinet Official / Area Superintendent	**Mark Shanoff – Interim, CIO**

Audit Result / Recommendation	**Management Response Acknowledgement / Agreement of Condition**	**Responsible Person (Name & Title) And Target Completion Date (MM/YYYY)**	**Management's Action Plan**
We recommend personnel in charge of selecting the vendors for any future interface with the Skyward system perform a due diligence in the form of a checklist and verify that the information they need from the vendor is gathered before entering in a contractual agreement. This will help to ensure no critical information regarding the interfaces is overlooked and help make an informed decision based on the information evaluated.	Agree with how it is written because Personnel in charge of selecting vendors reside in Procurement.	Pending	Vendor master data resides within Procurement per https://www.ocps.net/departments/procurement_services/vendors_and_community/vendor_registration/related_links. When procurement requests a checklist from OCPS divisions relative to vendors interfacing with district systems, we will comply with the direction provided to us from Procurement., as they maintain the master data for all vendors and contracts. Checklists should be memorialized within the statement of work which would reside in the contract, which is maintained and executed by Procurement Services. To that end, ITS finds the risk level tolerable given our current posture in the established vendor management processes.