Audit Committee Meeting

July 21, 2021 – 9:30 am - 450 Park Place – Conference Room 139

Attendees:

Rodney Jackson
Chris Ensslin (Audit Committee Chair)
Dave Osbourne (Audit Committee)
Larry Forester (Audit Committee)
Mark Sellars (Audit Committee)
Bill Kohm (Dean Dorton - Internal Auditor)
Kevin Cronwell (Dean Dorton - Internal Auditor)
Jim Tenza (Dean Dorton – Internal Auditor)
Jeanna Jones (Strothman – External Auditor)
Amy Greene (Board Member)
Bob Moore
Sherry Price
Lindsay Wright
Casondra Jones
All not in attendance are excused

Introductions & Approval of minutes – Chris Ensslin
Approved by Mr. Ensslin

Internal Audit - Dean Dorton
Bill Kohm gave introduction of his team.
Dean Dorton just completed their 2nd year at FCPS, now on the third audit cycle.
The Internal Auditors informed the committee that there were currently focusing on the Information Technology (IT) Audit, there were 7 observations (management comments) that will be walked through. Were on the back end of the Governance audit but wanted to give Dr. Liggins a chance to have some input to the feedback or response. They gave us a walk-through of the IT results. He discussed some areas that were looked at such as user awareness training, terminated user access removal administrator and super user access elevated privileges. No inappropriate access was noted. A recommendation was given that a formal schedule should be in place to look at all who have access with elevated privileges, should probably be done annually. Information was provided by Bob Moore who would be responsible and estimated completion date. There are less than 10 elevated privilege user's system wide, mostly consisting of the district systems people. Elevated access is being part of a security group within active directory. For example, a Teacher will have elevated access on the computers in the School's computer lab but will not have rights to their own or anyone else's in the District. Roles and rights should be reviewed throughout the District. The risk is more around personnel changes.
Safe Schools Learning Management System – Used to provide cyber security awareness training. Some of the training materials used are access to electronic media, using tech resources and FERPA to name a few. Recommendation has to do with email and messaging safety and were deemed to be inadequate. This module needs to be updated as it is very ineffective. IT is not a responsible for the content and

delivery of the training, it's a Human Resources and/or Risk Management function. IT goes through and selects appropriate technology related courses and to add to the module, IT must work within their system. The training consists of more than just IT courses, there are several other mandatory trainings included. There are better trainings available, but this course is better than nothing. All courses have quizzes at the end, but the email and messaging safety was not a very strong one.

Vendor Management – KDE relationship is a vendor management policy in draft mode with Dean Dorton supporting the recommendation that it is a high priority and should get it finalized sooner than later. We are responsible for protecting the data of our customers (parents, students, staff) as they expect to their data to be maintained at high standards. Using outsourced vendors bring in new risks. The type of data is part of the risk measurement. There are other forms of criticality such as availability. if we're getting offsite back-ups and allowing a vendor to manage them, then we're relying on that vendor to help with retrieval in the event of a disaster. It's not the volume of data that makes it high risk but the type of data. One element in the policy is that we will make an inventory of the vendors and rate their criticality and why. Most vendors will not need this type of policy and once cleaned up, the policy will give a more formalized processes and this will help reduce the risk to the vendors.
The question was raised if Payroll is outsourced? Answer: No, we use Munis (which the entire state is required to use) as our main finance system are other third-party vendors such as Frontline and Applitrack are these included on the types of things that's being discussed? Bob stated there has been a list started which includes criticality in two different areas, Business Continuity and Data Security. We have around 150 cloud vendors, so when looking at Munis and Infinite Campus these are critical to our business operations but also with data security as this contains confidential information. So even though we are required to use Munis and IC they are still tied for number 1 on our critical vendor list. Munis does an annual disaster recovery test, we need to hold our other critical vendors to the same type of standards.

Question was asked, If Munis offers something like other systems we use such as Frontline and others, should we be utilizing the Munis software instead for security? From an IT standpoint, It was suggested that fewer numbers of vendors lower our risk, as information is in fewer places. However, that would be an HR decision and hopefully we would be part of that. As we consolidate into a Munis type system where they use modules, we lower our risks. Those are the types of business decisions are where it's good to have IT involved in so they can raise flags on risks that may need addressing. Recommendation is to review inventory of critical third-party hosting organizations being utilized. The policy will address two things, one is evaluating vendors and the need for recurring evaluations. The number one thing we are addressing right now is not just in the vendor management procedure but also in the procurement procedures to try and get some boilerplate language in the RFP process that either reference the vendor management process or puts the annual reviews into the RFP process as part of what we do as part of our procurement process.

Mr. Jackson asked - Should part of the standard operating procedure state that when using a third party the Technology team is involved as a big concern is that Munis could do the job of several systems we use but there is no consultation during the RFP process? Mr. Moore responded that there will be a vendor management committee that includes Financial Services, Munis, IT and whole range of others across the District. Will the policy have a Munis and non Munis sections on it? Munis will be a critical

application based on the criticality of the vendor, the reviews will be different. There will be a level 1 critical system (Munis and IC are among those that will fall into that) so for that level there will be an annual disaster recovery system. Level 1 deals with safety, communications, transportation, and payroll. Level 2 may be something like Frontline (hiring tool). KDE – Manages the Districts firewalls. It's a shared environment with information from other districts and they're hesitant to give too much visibility. Recommendation that KDE provide evidence they're doing vulnerability scans and penetration testing on the firewall. We need to have a process in place that has KDE provide this information. IT agrees with this and they're considering creating a Network System Admin position to be responsible for security related issues. The person in this position would be like a traditional security officer (things looked for in this audit). We need to know from KDE if controls are in place to make sure data is secure, an agenda item is needed to address this. Does KDE have an audit to look at their firewall? They do but they do not provide much information. We would do penetration testing on KDE's equipment that would be managed by our security officer but done by a third party (someone without knowledge of our system to try and break through and find vulnerabilities but nothing destructive).

Active Directory – Computers in the environment – Based on older computers we found a list of Operating Systems not being supported by Microsoft and no longer receiving patches. Recommendations is to purge outdated information, old computer accounts. Out of the 200+ found, about half of the computer accounts have been disabled and about 20 of the others are HVAC control system that were updated over the summer. This one should be taken care of quickly.
Active Directory Password Settings – Significant areas for improvement. Effective July 1st password character limit requirement was increased to 15, anything 10 or above is a minimum for today's vulnerabilities, password history is now remembered and Office 365 has an account lockout function so after too many incorrect password attempts the account gets locked for a certain length of time. From the local active directory there needs to be a failed login attempt on that as well (probably 5 times). Passwords need to be changed every six months or a trigger will prompt a password change. Recommendation is to have a 15-character pass phrase length, set number of failed logins attempts and six-month password expiration. Passwords or pass phrases need to be strong.

Removing User Access –Resignations, non-renewals and After School part time staff have different procedures. Example of process breakdown, someone retired but came back to be After School part time staff resource and their termination never got properly processed. This was a low risk. Recommendation is there needing to be a standardized process for things different than normal terminations. IT and HR need to work together to identify a practical and effective approach. Question related to this, if someone gets a non-renewal in April and becomes a disgruntled employee but is still under contract until June and are still working and have access to the system, can't they do a lot of damage? There have been very few cases where an employee is expected to become disgruntled, their access is manually reduced, however, there are legal implications on that situation. Most of those positions are Teacher's without access to critical systems, but some could be Bookkeepers with Munis access too. These situations would be up to the Building or Department Leader to handle. There are a lot of checks and balances that can be done, if they do damage the system.

Governance Audit is basically done but wanted to make sure Management properly responds to the findings. Bill Kohm shared some insight for a book called Governance Core of School Boards, Superintendents and Schools Working together as an excellent read.

What to look forward to in October, already started Payroll Audit. Suggested to look at user access communication, to see about the terminations that were discussed, however, that's part the HR side of things.

- FY22 - Base Audit Schedule
- July 2021 - IT Audit 2022 Audit Plan
- Oct 2021 - Payroll Audit (in process), Governance, Risk Assessment
- Jan 2022 - IT Audit, After School Audits
- April 2022 - Transportation Audit (met with Myron Thompson about this)

They have been able to stay within the budget of $100,000.

External Audit – Strothman

They've already had the Initial planning meeting with management for the 2021 FY Audit. They've started receiving some of the planning type documents for working through the single audit to start making sample selections and hope to have done by the end of the month. Beginning in August, school visits will start. They have received audit packets from some Bookkeepers but are still waiting several more. Excited to be back again and will have an update in October. The External Auditors are hoping to be done with most of the work other than just tidying up the financial statements by October.

Compliance Report - Lindsay Wright

The hotline is still up and running. No new reports or complaints have been made through the hotline since the last report. Hotline will continue to be monitored. With the new school year starting, Lindsay will be doing a harassment, discrimination, and grievance process presentation for staff with information about the hotline included. There was an investigation conducted along with Financial Services involving a situation that occurred at a high school that's important to note. The investigation began in May and was completed last month. Lindsay worked with Financial Services and Human Resources. School level support was provided as well as district level school chief. It was investigated from a personnel and legal perspective. There was administrative action taken with at least one staff member with other financial findings. There were no missing funds. Some fixed assets were disposed of that should not have been. Auditors were notified and on standby if needed. Cindy Hipsher and Lindsay worked together simultaneously but separately with one another. The school in question is on the list to be audited this year.

Audit Committee Miscellaneous Requests and Comments

Sharon Holbrook has resigned as Audit Committee vice-chair, will be looking for her replacement.

Next meeting will be in person, at 9:30 am

Motion to adjourn by Larry Forester, seconded by Dave Osbourne