Longwood Central School District

Review of Access Permissions

2015-2016 School Year

Presented to the Audit Committee October 6, 2016

October 6, 2016

Board of Education
Longwood Central School District
35 Yaphank Middle Island Road
Middle Island, NY 11953

Board of Education:

We have been retained to function as the internal auditor for the Longwood Central School District (hereinafter, "the District"). Our responsibility is to assess the internal control system in place for the accounting function within the District, and to make recommendations to improve upon certain control weaknesses or deficiencies. In doing so, we hope to provide assurance to the District's Board, management, and residents, that the fiscal operations of the District are being handled appropriately and effectively.

BACKGROUND AND OBJECTIVE:

In our Initial Risk Assessment report dated March 2015, we recommended examining the specific access and administrative rights to key applications such as Finance Manager (financial management system), Power School (student management system), and IEP Direct (special education management system), to ensure there is adequate segregation of responsibilities. Access controls are intended to provide reasonable assurance that computer resources are protected from unauthorized use and modifications. To control electronic access, a computer system or application needs a process to identify and differentiate among users. User accounts identify users and establish relationships between the user and a network, computer, or application. The system administrator creates these accounts. These accounts contain information about the user, such as passwords and access rights to files, applications, directories, and other computer resources. The objective of our audit was to determine whether access rights to these applications was appropriately assigned.

SCOPE AND PROCEDURES PERFORMED:

To perform this evaluation, we gained an understanding of how access is granted and then verified that the access permissions within each of the three applications is properly restricted, that proper segregation of duties exists, and that access is limited based on the user's job descriptions and responsibilities. The results of this review are documented below. Specifically, we verified the following:

I. FINANCE MANAGER

We obtained a report of all users' access permissions within Finance Manager as of April 4, 2016. Finance Manager contains several modules for performing various financial and human resources functions. The District utilizes the following modules:

- Accounting – purchasing, cash disbursements and payments, budget transfers, journal entries, cash receipts.
- Budgeting – budget development and "what-if" scenarios.
- Human Resources – personnel management (employee attendance, appointment earnings, fingerprint information, health benefit information), professional management (tenure and certification information)
- Payroll – contract earnings, employee deductions, retirement contributions, paychecks.
- Negotiations – centralizes employee contract salaries for negotiation, creation of salary schedules.
- Requisitions – creating and approving purchase requisitions.
- System Manager – ability to add/change/delete access permissions within modules (access to this module should be restricted and limited to a few management personnel).

Finance Manager has the ability to produce a log indicating when, where, and who uses the computer system. It can also generate a log of all changes made to the information included in the vendor master files. Because virtually all District accounting records and reports are computer generated, it is important that District officials review audit logs periodically. Without such a review, the District does not have adequate assurance that changes to its financial information are appropriate and authorized.

Finance Manager allows the District to specify the level of auditing that is to take place as transactions are entered, updated, and deleted in the system. There are three settings of audit logging that the District can set:

- **Low**: the audit process is restricted to selected monetary-related tables. Activities related to maintenance of absence, appointment, assignment, deduction, payroll calendar, pay schedules, projections, seniority entry, user maintenance, and vendor maintenance are the types of transactions that are audited when setting the Audit Policy to Low.
- **Medium**: Along with the activities specifically mentioned above under Low, the system will audit the following types of transactions: maintenance to any of the system codes (attendance codes, certification codes, certification types, etc.), cash disbursement/receipt maintenance, purchase order maintenance, PR emergency contact/dependent maintenance, requisition maintenance, etc. With this setting, the system **WILL NOT** audit any of the global utilities, such as projections move to payroll, payroll calculation, etc. Finance Manager recommends that districts utilize this logging setting.
- **High**: In addition to the user activities mentioned above, the system will audit **ALL** database activities, including global utilities such as the earnings move to payroll, payroll calculation process, change deduction amounts/limits, etc. This setting is generally not recommended, as this type of audit logging has a significant impact on system performance.

> We noted that the District's audit logging is currently set to "medium", which is the recommended setting. In addition, we noted that the payroll edit logs are reviewed by the Superintendent on a regular basis. **No exceptions were noted**.

Users are assigned access to specific menus within each module. The menus are correlated to specific functions that can be performed within the system, and are categorized as a report, maintenance, utility, or data entry function. Access to each menu function can be restricted by the ability to add, update, delete, and/or print. Permissions are granted once the request for access is completed, reviewed, and approved by the Assistant Superintendent for District Operations. The access permissions in Finance Manager are entered by select staff in the technology department.

Utilizing the Finance Manager report of all users' access permissions, we analyzed those individuals who have add, update, and/or delete privileges within each menu that was categorized as a data entry function. A total of 28 of 334 users were selected and their access permissions further analyzed. Based on the access capabilities listed, we assessed if the permissions granted are those functions needed to perform within the selected employees' job duties, and that each employee is restricted from performing multiple aspects of a financial transaction that could compromise proper segregation of duties. In addition, we selected 15 Finance Manager Access Request forms and compared the access permissions in Finance Manager to those permissions indicated on the form. **No exceptions were noted**.

> **<u>Auditor's Comment</u>**: We noted that Eastern Suffolk BOCES has full access to Finance Manager as they are assisting the District in the process of upgrading the version of Finance Manager to nVision. To strengthen the access controls within Finance Manager, the District should periodically monitor the activities performed by Eastern Suffolk BOCES to ensure that access is appropriate.

II. POWER SCHOOL

Power School is the District's student management information system, and is utilized for creating student schedules, tracking student attendance and enrollment, recording student grades, and creating student transcripts. This system links with IEP Direct (special education) and WinSNAP (food services).

Users are assigned access to specific groups that allow the user to perform specific functions within Power School (e.g. a group may only have "view" capabilities). The groups are correlated to a set of specific activities that can be performed within the system. Access to each activity can be further restricted by the ability to view or modify data based on need, such as restricting a teacher's access to only current year students.

The District established 35 access groups (e.g., registrar, counselors, attendance, health, teachers, department chairs, building administrator, etc.) that allow access to be restricted to specific functions as well as the type of access that the user can perform (i.e. view only or modify). For teachers, the system administrator assigns access to only the current students' records assigned to that teacher based on current year schedules. Students are given access to Power School based on current enrollment. Each student is placed in a student user group and the student only has access to their own records.

Power School produces audit logs that capture when a person accessed the system and what accesses were performed within the system. This enables the system administrator to run various reports to monitor access to the system as well as changes to specific data including changing grades and attendance records. The system administrator reviews the audit/edit logs on a regular basis throughout the school year, and will follow up with District management if discrepancies or anomalies are noted during the review. We did note that Power School permits the database to be exported and imported by those with system administrator access. We confirmed that any changes made to the exported data are logged and are subsequently reviewed when the data is imported back in to the main database.

Utilizing the report of all users' access permissions as of April 12, 2016, we analyzed the individuals assigned within each group. From the list of users within each group, we assessed if the permissions granted are those functions needed to perform their job duties, and that the employee is restricted from performing actions that could compromise proper segregation of duties (i.e., a teacher being able to change a grade after the grade has been finalized). We also verified that access was limited to only current students to address Family Education Rights and Privacy Act (FERPA) compliance stipulations.

> **Issue #1**: We noted that controls over access within Power School can be strengthened. Due to the sensitive nature of this information, specific vulnerabilities are not discussed in this report but have been communicated to District officials so they can take corrective action.
>
> **Risk**: There is an increased risk of unauthorized access.
>
> **Level**: Moderate - High
>
> **Recommendation**: We recommend that the District strengthen the access permissions within Power School.
>
> **Auditor's Comment**: We noted during our review that Power School does not automatically link and update the District's transportation software, Versatrans. We were informed that there are some incompatibilities with respect to the method the student's address information is maintained between the two software applications. As such, the District has to manually enter any additions or revisions to a student's demographic information in Versatrans and Power School. To improve efficiencies, the District should evaluate and assess whether this process can be automated.

III. IEP DIRECT

The software application, IEP Direct, enables the District to document and track special education services provided to District students. This system utilizes the database information from Power School (e.g., student class lists) allowing data to be integrated automatically. Data is shared between IEP Direct and Power School through the Schools Interoperability Framework (**SIF**) compliance feature within IEP Direct. The District utilizes Centris Sync to import demographic information directly from Power School, and as such, these changes can only be made in Power School. Changes made to the student's IEP are based on the recommendations from the CSE and are reviewed by the staff responsible for the student's IEP before the IEP change is finalized. The IEP cannot be changed except by the systems administrators. Actions performed within IEP Direct automatically track the user ID and the date of access. IEP Direct has several reporting features that enable the District to verify the records.

The District established 3 main groups to ensure access to the student records is appropriately restricted:

- Central Office - includes staff such as special education chairpersons and supervisors, the District attorney (on an as needed basis), and psychologists;
- School Building – includes staff such as principals, assistant principals, social workers, deans, and nurses; and
- Student Level – includes special education teachers as well as other support service staff such as occupational therapists.

Within each group, users are further grouped according to their job function and are restricted to view only /edit of certain records (e.g. a special education teacher only has access to those students assigned to the teacher's class). Utilizing the report of all users' access permissions, we analyzed the individuals assigned within each group. Based on the list of users within each group, we assessed if the permissions granted are those functions needed to perform their job duties, and that the employee is restricted from performing actions that could compromise proper segregation of duties (i.e. a teacher being able to change an IEP of a student that is not assigned to them).

> We obtained a report of all users' access permissions within IEP Direct as of April 11, 2016. We reviewed a sample of 35 user names from the list of users within all the groups and verified that access to IEP Direct was appropriately requested and the user was assigned to the correct access group. Based on our review, the access permissions within IEP Direct are appropriately assigned, and the accesses granted are based on job functionality. **No exceptions were noted**.

We would like to thank the staff at the District for their cooperation and professionalism during our testing.

We understand the fiduciary duty of the Board of Education, as well as the role of the internal auditor in ensuring that the proper control systems are in place and functioning consistently with the Board's policies and procedures.

Should you have any questions regarding anything included in our report, please do not hesitate to contact us at (631) 582-1600.

Sincerely,

Cerini & Associates LLP

Cerini & Associates, LLP
Internal Auditors