

**Cold Spring Harbor Central School  
District**

*Internal Audit Report on  
Information Technology*

Cold Spring Harbor Central School District  
Internal Audit Report on Information Technology

**TABLE OF CONTENTS**

	<u>Page</u>
Report on Internal Controls Related to Information Technology	
Network and Network Security	1
Accounting Information System	2
Other Applications	3
Information Technology and Disaster Recovery Plan	4
Findings and Recommendations	5 - 7
Corrective Action Plan	8

Board of Education  
Cold Spring Harbor Central School District  
75 Goose Hill Road  
Cold Spring Harbor, NY 11724

We have been engaged by the Board of Education (the "Board") of the Cold Spring Harbor Central School District (the "District") to provide internal audit services with respect to the District's internal controls related to information technology for the period July 1, 2012 through January 30, 2013.

The objectives of the engagement were to evaluate and report on the District's internal controls pertaining to information technology and to test for compliance with laws, regulations, and the District's Board policies and procedures.

In connection with the following procedures, we have provided findings and recommendations for the internal controls related to information technology. Our procedures were as follows:

- Reviewed the District's policies, procedures, and practices with regards to the internal controls related to information technology;
- Interviewed key District employees involved in the information technology processes;
- Performed a physical observation of the District's server rooms in the Goosehill Primary School and the Cold Spring Harbor Junior/Senior High School to verify the server rooms were properly secured and that the servers were reasonably protected from fire and floods;
- Reviewed the user permissions within the accounting information system to identify multiple active user accounts, generic user accounts, and possible permissions granted to various employees that may not be consistent with their job responsibilities;
- Performed a comparison of the master vendor file to the master employee file to identify possible conflicts of interest;
- Reviewed the master vendor file to verify that the master vendor file was complete, accurate, free of duplicate vendors, and up to date; and
- Reviewed the District's Disaster Recovery Plan to determine that the Plan identified critical information technology infrastructure and equipment, established the most suitable recovery strategy for each application utilized by the District, and identified those individuals responsible for overseeing the disaster recovery process.

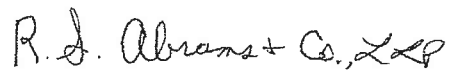
The results of our procedures are presented on the following pages.

Our procedures were not designed to express an opinion on the internal controls related to information technology, and we do not express such an opinion. As you know, because of inherent limitations of any internal control, errors or fraud may occur and not be prevented or detected by internal controls. Also, projections of any evaluation of the accounting system and controls to future periods are subject to the risk that procedures may become inadequate because of changed conditions.

We would like to acknowledge the courtesy and assistance extended to us by personnel of the District. We are available to discuss this report with the Board or others within the District at your convenience.

This report is intended solely for the information and use of the Board, the Audit Committee and the management of the District and is not intended to be and should not be used by anyone other than those specified parties.

Very truly yours,

A handwritten signature in cursive script that reads "R.S. Abrams & Co., LLP".

R.S. Abrams & Co., LLP  
March 22, 2013

## **NETWORK AND NETWORK SECURITY**

### **Firewalls and Intrusion Detection Systems**

A firewall is used to implement access control between two networks. It allows the District's network users to access outside information while preventing those outside the District from accessing the District's systems. The District's firewall consists of a combination of hardware and software that provide several layers of protection against intrusions.

### **Physical Security**

The District's Network Operations Center ("NOC") is currently at the Cold Spring Harbor High School. In addition to the NOC there is a server room located at the Goosehill Primary School. All server rooms are temperature controlled and uninterrupted power supply ("UPS") units are in place to protect the District's equipment from an unexpected power disruption that could cause business disruption or data loss. In addition, the District has converted most of its physical servers to virtual servers.

### **Back-up Controls**

The District utilizes many virtual servers that back up to each other several times throughout each day. In addition, all user files for employees of the District are backed up twice a day by performing "shadow copies". Emails are archived by BOCES daily and can be accessed for up to seven years. The District also contracts with an outside vendor to backup the *Finance Manager* data nightly and stores it in two offsite locations.

### **Network and Email Access**

Microsoft Exchange serves as the District's email server and the District uses *Active Directory* for the authentication of email and network users. All access requests, changes to user permissions, additions of new employees and removal of terminated employees from *Active Directory* are executed by the Director of Technology or one of his two technicians.

### **VPN**

A virtual private network ("VPN") is a network that allows remote users to securely access the District's network using a public telecommunication infrastructure, such as the Internet. In addition to users being granted access from time to time, *Finance Manager* has VPN access. However, this access is limited to the *Finance Manager* server only. When *Finance Manager* needs VPN access to perform server maintenance, they must contact the Director of Technology to establish a window of time for performing maintenance. *Finance Manager* will then be granted VPN access for the agreed upon period of time and when this time expires, access will be terminated.

### ACCOUNTING INFORMATION SYSTEM

The District utilizes *Finance Manger* as its Accounting Information System (“AIS”). This application was installed by *Finance Manager* and requires *Finance Manger* to perform application updates, database management and, if necessary, system restores. The following modules of *Finance Manager* were identified as being utilized by the District (a description of the modules has been provided):

- ***Accounting Manager*** – Maintains general ledger, accounts payable, budgetary accounting, receipts/revenue, encumbrances/purchasing, project/grant accounting; generates financial documents such as computer-generated checks, purchase orders, account and vendor histories, and assists with controls to maintain data integrity and balanced entries.
- ***Budget Manager*** – Assists in the annual budget preparation.
- ***Human Resource Manager*** – Maintains all employee data, including detailed attendance histories, benefits tracking, educational and PDP credits, observations and evaluations, fingerprint tracking, retirement data and emergency medical information.
- ***Negotiation Manager*** – Creates salary matrices to maintain contract salaries and hourly rates for all personnel. Constructs salary schedules with multiple steps/levels for development of numerous contract scenarios for simple comparison.
- ***Payroll Manager*** – A payroll generation program that provides detailed employee records and custom generation of payroll.
- ***Receivables Manager*** – Provides all relevant financial documents: invoices, billing journals, aging reports, reminder notices, customer histories and revenue source journals.
- ***Requisition Manager*** – Enables individuals throughout the District to electronically submit purchase requisitions and allows for electronic approval of requisitions submitted.

#### Passwords

The District should have procedures in place to periodically verify its system of controls are working as intended, are still needed, and are cost effective, including a review of the controls over access to information systems. Access to computerized files and transactions should be restricted to authorized individuals only. This can be accomplished with the use of passwords and software that restricts users' access and can help ensure that only authorized individuals utilize the computer system.

#### Permissions

A good internal control framework requires District management to develop a system of controls that includes proper segregation of duties in the District’s operations. A proper segregation of duties should exist not only in manual processes, but also within the AIS. *Finance Manager* allows the system administrator, the Director of Technology, to restrict access to functions specific to job descriptions.

**OTHER APPLICATIONS**

**eSchoolData Systems**

*eSchoolData Systems* (“*eSchoolData*”) is the student data management application currently utilized by the District, which allows the District to track attendance, behavior, and grades by student. The system also provides a course catalog, graduation planning, a grade book, and assists the District in preparing required reports submitted to the New York State Education Department. The entire system is web-based, which allows teachers, instructional administrators, instructional clerical staff, and parents to access student information. Further restrictions are applied to the individuals’ user privileges to ensure that only authorized users are seeing specific information (i.e. teachers only have access to enter attendance and grades; all other functions are restricted).

**IEP Direct**

*IEP Direct* is the special education student management application currently utilized by the District. *IEP Direct* is a web-based application that is used in conjunction with *eSchoolData*, to track student IEP’s, evaluations, meetings, and assists with the preparation of New York State required reports. Additionally, *IEP Direct* enables the preparation of STAC forms, facilitating the recovery of Medicaid funds. The system has an optional Medicaid Direct add-on that automates the Medicaid tracking and billing process for maximizing revenue recovery by improving data accuracy and accelerating collections. *IEP Direct* also facilitates District compliance with applicable privacy laws and regulations.

## **INFORMATION TECHNOLOGY AND DISASTER RECOVERY PLANS**

### **Information Technology Plan**

The purpose of the District's *Technology Plan* is to define and outline the steps necessary to prepare students for challenges and opportunities in their educational endeavors by providing the best possible technology environment. The District's *Technology Plan* discusses the District's plans for architecture, hardware, software, staff training, implementation, and evaluation. The current Technology Plan covers a three-year period from 2012 through 2015.

### **Disaster Recovery Plan**

Disaster recovery planning is a subset of a larger process known as business continuity planning and includes planning for resumption of applications, data, hardware, communications (such as networking), and other information technology infrastructure. While the District would like to ensure zero data loss and zero time loss in the event of a disaster, the cost associated with that level of protection may be impractical.

The District's adopted *Comprehensive Data Backup and Disaster Recovery Plan* is comprised of several sections that document the procedures and resources that are to be followed and used in the event that a disaster occurs at the District. The sections of the *Comprehensive Data Backup and Disaster Recovery Plan* are as follows:

- Introduction;
- Data in Order of Importance;
- Hardware/Software;
- Server Backup Procedures;
- Security of Financial Database; and
- eSchool Data Knowledge Management System



## **FINDINGS AND RECOMMENDATIONS**

Based on our interviews, observations, and detailed testing, we have provided our findings and recommendations below to further strengthen the District's internal controls as they pertain to information technology outlined above.

It should be noted that these recommendations are provided to the District to assist management in improving the District's internal controls and procedures relating to information technology. It is important to note that our findings and recommendations are directed toward the improvement of the system of internal controls and should not be considered a criticism of, or reflection on, any employee of the District.

### **Policies and Procedures**

Procedure Performed: We reviewed the District policies to determine whether the District has adopted the legally required policies with regards to information technology.

Finding: No exceptions were found as a result of applying this procedure.

\*\*

Procedure Performed: We reviewed the District's procedures with regards to the internal controls related to information technology.

Findings: We noted that the District does not periodically review audit trail reports within *Finance Manager* for user activity to identify any activity that appears to be unusual. Additionally, we noted that the District does not review the login/logout report within *Finance Manager* to identify users who may be logging into the financial software at unusual times.

Recommendation: We recommend that the District implement procedures to review audit trails. We also recommend that the District periodically review the login/logout report within *Finance Manager* to ensure users are not accessing the financial software at unusual times. Additionally, we recommend that these reviews are documented and maintained on file within the business office.

\*\*\*

### **Server Rooms**

Procedure Performed: We physically inspected the District's server room in the Goosehill Primary School and the NOC located in the Cold Spring Harbor Junior/Senior High School to verify the server room is properly secured and that the servers are reasonably protected from fire and floods.

Findings: We noted that the NOC does not have fire detection systems in place as required by the National Fire Protection Association *Standard for the Protection of Information Technology Equipment* (NFPA 75). We also noted that the temperature must be regulated manually by

Cold Spring Harbor Central School District  
Internal Audit Report on Information Technology

District personnel and that there is no warning system to notify them if the temperature exceeds the recommended level.

Recommendations: We recommend that the District install a fire detection system in the NOC, at a minimum, to be compliant with the National Fire Protection Association *Standard for the Protection of Information Technology Equipment* (NFPA 75). We also recommend that the District either install a temperature monitoring system or put procedures in place to regularly inspect the temperature inside the NOC.

\*\*\*

**Finance Manager Permissions**

Procedure Performed: We reviewed the user permissions within *Finance Manager* to identify multiple active user accounts, generic user accounts, and possible permissions granted to employees that may not be consistent with their job responsibilities.

Finding: We noted that the District has not restricted the ability to delete or modify journal entries within *Finance Manager*. Deleting transactions will cause a break in the transaction sequence, and a partial deletion of the physical audit trail.

Recommendation: We recommend that the District disable the ability to delete or modify journal entries within *Finance Manager* for all users. If a transaction deletion occurs, the District should document the reasons in order to maintain a full audit trail.

\*\*

Finding: We noted one individual who has two active user accounts within *Finance Manager*.

Recommendation: We recommend that the District ensure that each individual who has access to *Finance Manager* be given only one active user account.

\*\*

Finding: We noted that the Interim Assistant for Business, Director of Technology, Finance Manager, accounts payable clerk, District Treasurer, Account Clerk Typist in Buildings and Grounds, and the Account Clerk Typist in the Registrar office have override capabilities with no limit.

Recommendation: We recommend that the District establish a more reasonable limit for overriding purchase orders, cash disbursements and the general ledger to improve controls surrounding the District's budgetary management and reduce the risk that budget lines will be over expended.

\*\*

Findings: We noted the following example of segregation of duties violations within *Finance Manager* where District employees have been granted incompatible duties by having access to functions not pertaining to their job description:

- The Interim Assistant for Business, Director of Technology, and Finance Manager have the ability to post budget transfers and budget adjustments;

Cold Spring Harbor Central School District  
Internal Audit Report on Information Technology

- The Director of Technology has the ability to perform journal entries; and
- The Interim Assistant for Business, Director of Technology, Finance Manager, and the Account Clerk Typist in the Registrar office have the ability to perform cash receipts;

Recommendation: We recommend that the District review its current permissions in *Finance Manager* and create a system of controls that ensures the proper segregation of duties and restrict access where necessary. In addition, if an employee functions as a backup to another employee, permissions should be temporarily granted and then taken away as needed.

\*\*\*

**Vendor/Employee Match**

Procedure Performed: We performed a comparison of the master vendor file to the master employee file to identify possible conflicts of interest.

Finding: No exceptions were found as a result of applying this procedure.

\*\*\*

**Vendor Master File**

Procedure Performed: We reviewed the master vendor file to verify that the master vendor file is complete, accurate, free of duplicate vendors, and up to date.

Finding: No exceptions were found as a result of applying this procedure.

\*\*\*

**Disaster Recovery Plan**

Procedure Performed: We reviewed the District's Disaster Recovery Plan (the "Plan") to determine that Plan identifies critical information technology infrastructure and equipment, establishes the most suitable recovery strategy for each application utilized by the District, and identifies those individuals responsible for overseeing the disaster recovery process.

Finding: No exceptions were noted as a result of applying this procedure.

Cold Spring Harbor Central School District  
Internal Audit Report on Information Technology

**CORRECTIVE ACTION PLAN**

The District is required to prepare a corrective action plan in response to any findings contained in the internal audit reports. As per Commissioner's Regulation §170.12, a corrective action plan, which has been approved by the Board, must be submitted to the State Education Department within 90 days of the receipt of a final internal audit report.

The approved corrective action plan and a copy of the respective internal audit report should be sent to the following address:

New York State Education Department  
Office of Audit Services, Room 524 EB  
89 Washington Avenue  
Albany, New York 12234  
Attention: John Cushin