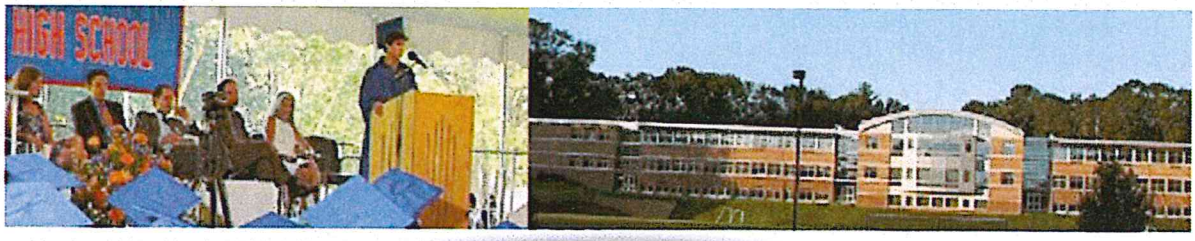


a community for learning

Chappaqua Central School District

Intensive Review of Information Technology

Covering the State mandate for the year ending June 30, 2013

Chappaqua Central School District

Table of Contents

TOBIN & COMPANY
CERTIFIED PUBLIC ACCOUNTANTS, PC

To the Board of Education of the
Chappaqua Central School District
Chappaqua, New York

We have performed an intensive review in the area of Information Technology for the Chappaqua Central School District (the District). The purpose of this engagement is to ensure compliance with applicable New York State laws and regulations under the Fiscal Accountability Initiative for the fiscal year ended June 30, 2013.

Our report provides results of attribute testing performed on the selected area. In addition, our report indicates any areas for which we believe improvements can be made to existing processes and internal controls.

We are pleased to have had the opportunity to serve you and look forward to reviewing this report in detail with you. We would also like to thank the Board of Education and the employees of the Chappaqua Central School District for their time and assistance during our engagement.

Sincerely,

Tobin & Company
Certified Public Accountants, PC

Larchmont, New York
December 28, 2012

2001 PALMER AVENUE • LARCHMONT, NEW YORK 10538 • TEL: (914) 833-2200 • FAX: (914) 833-2278

Intensive Review

At the request of the Audit Committee of the Chappaqua Central School District ("the District") we have performed an intensive review of the District's Information Technology ("IT). Our review of Information Technology included, but was not limited, to the following procedures:

1) Detailed interviews of District personnel and documentation of these interviews through industry accepted checklists.
2) Review of the District's disaster recovery plan and backups.
3) Review of District policy and procedures over emails.
4) Review of District policy and procedures over internet usage.
5) Review of physical security of servers, equipment and software.
6) Review of District network configuration and access to network.
7) Review of Finance Manager Access rights.
8) Review of software licensees and equipment warranties.
9) Review of backup process at Regional Information Center (RIC).

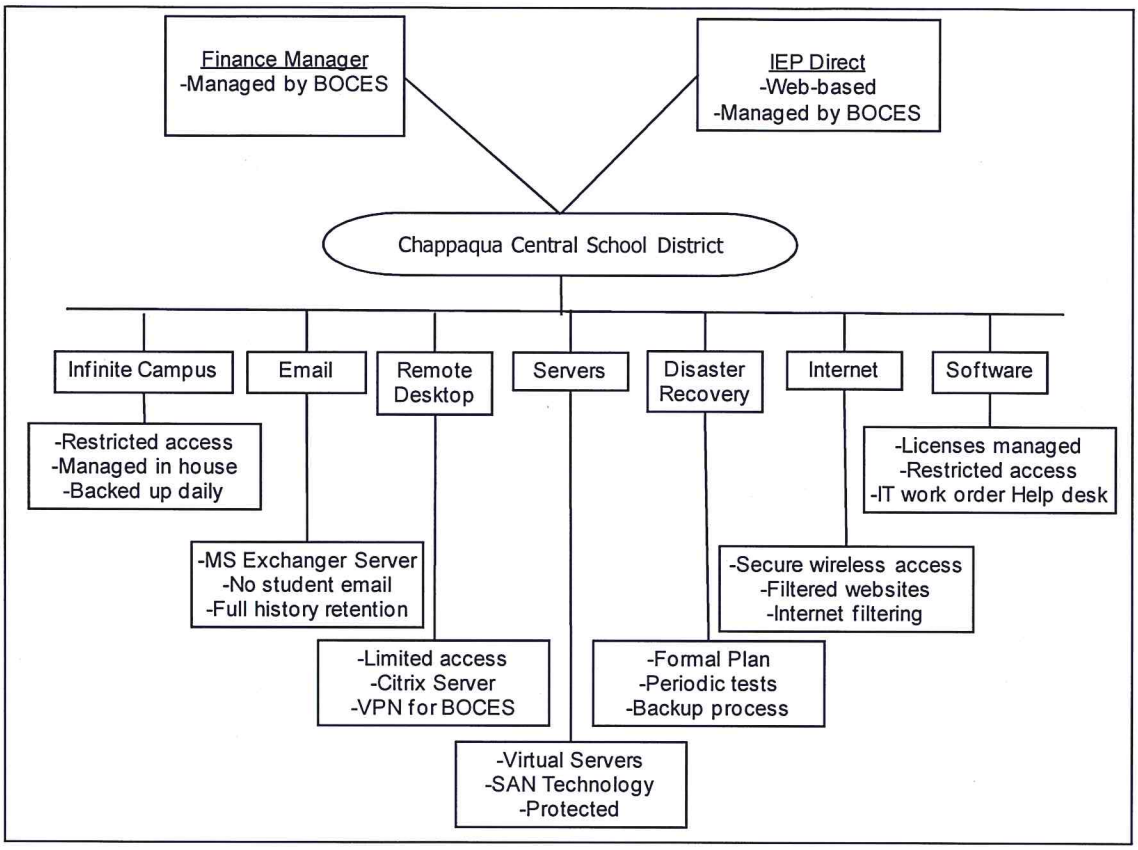
The objective of our review was to provide the District with an objective review of IT and to identify any areas of weakness and areas for potential improvement. The District's management is responsible for the District's IT operations, and for the development and implementation of related internal controls.

Key personnel interviewed during our process were as follows:

- Director of Information Technology, *Darleen Nicolosi*
- Network Engineer/Administrator, *John Louch*
- Network Technician/lead support, *Howard Giebel*
- Assistant Superintendent for Business, *John Chow*
- District Treasurer, *Blanche Blair*

Summary

Technology Overview



Notable observations

1) Good management of network environment.
2) Network well designed and separated.
3) Knowledgeable IT staff.
4) Formal disaster recover plan established.
5) Modernization to virtual servers.
6) Good internet filtering, secure wireless access.
7) Well developed technology plan for future projects.
8) Complex passwords are used.
9) Servers are secure and protected from elements.
10) Equipment is tracked and inventoried.
11) Well established backup and storage.
12) Good management of software licenses.
13) Updates and patches are done periodically.

Observations for potential improvement

1) Review of copier and fax disposal policy.
2) Establish individual administrator log ins.
3) Consider vulnerability scans on firewalls.
4) Perform firmware updates more often.
5) Assign a second emergency contact.
6) Establish a plan for excess monitors.
7) Utilize snapshot technology on SAN server.
8) Perform full recovery tests on critical systems.
9) Establish a DMZ on Citrix and Exchange server.
10) Review chat room policy and access.

The following details our understanding of policies, procedures, and controls in place over various aspects of the Districts information technology.

General

The District is contracted with New England System and Software (NESS) to provide technology (IT) support staff. The District currently has 7 specialists from NESS that perform various levels of IT duties, and report directly to the Director of IT. Most of the IT staff from NESS has been with the District for over 10 years. Each staff member is crossed trained and can perform various duties if needed. NESS services other school districts as well as some NYS government agencies and meets with other school district IT counterparts to stay abreast of industry changes.

The District has a set of policies and IT procedures in place to ensure the District's employees, students and IT staff use and perform their tasks in a consistent and approved manner. Any person using the District's IT must read and sign the District's "acceptable use policy". The District has a formally documented technology plan and disaster recovery plan which details the policies and procedures in the event of an unforeseen disaster.

The District has established a 3 year technology plan, which outlines future goals and hierarchy of projects. In addition to working on major projects, the IT staff regularly assists District users with support, both for hardware and software issues. The IT staff utilizes a help desk work order system "Help Star". Users with problems or questions can contact the staff via email or phone and communicate their issue. This work order system is an excellent tool in managing and tracking jobs as well as indentifying common problems.

Areas for potential improvement:

1) Observation: Copiers and fax machines have built in hard drives that store information each time they are used. When the machine is returned to the vendor or disposed, the information may be accessed by an unauthorized person.
   Recommendation: The District should review its copier contract to ensure the hard drive information is destroyed or permanently deleted.

Conclusion

The District's IT structure is similar to that of other school districts. We found similarities in internet restrictions, wireless access, security measures, network access and software and hardware equipment. The most notable difference is the District's move towards server virtualization which is ahead of many other districts we have visited. The other difference is the contracted IT support through NESS instead of BOCES. Although, many school districts use BOCES to provide their IT support we feel NESS provides a similar level of expertise and service. We believe the District's Information Technology is secure and on par with other school districts.

Network administration

Overall we felt the student and administrative networks are carefully designed and managed. The District has a good separation and security of its network domains. Providing separate domains for students and administration provides an additional layer of security to District resources. There is no device to device connection on the networks which eliminates the risk of one computer compromising another.

There are four main network systems of the District; Infinite Campus, which maintains the student and teacher information database, IEP Direct, which maintains all special education information, Finance Manager, the finance program of the district, and the Internal Network maintained by the IT Department.

The network is separated by two domains; Curriculum and Administration. Students and faculty are assigned to the Curriculum domain, and administrators and faculty may be assigned to both the Administrator domain and Curriculum domain. Each user has certain access to the network files based on predetermined user rights. Each employee has a profile which determines what files and applications they will be able to access when they log in. In order for an employee to obtain additional access rights, a signed request must be made by the department chairperson. Students are given access to the "H Drive" to save their documents and the "S Drive"; the purpose of which is to be able to share documents with teachers and other students. In addition to "S Drive" teachers also have access to "T Drive" which is used to share documents and resources between other teachers and administrative staff. Since all users are set up with profiles, and all documents are stored on the network, they can log into any computer and pull up their documents without having to work from the same computer each time.

The District network comprises of 1 firewall and 1 router which are managed by the District's IT staff. The District has a subscription with SMARTnet that provides up to date patches, virus definitions and service packs. The firmware on the firewalls, routers and switches are updated annually.

Areas for potential improvement:

1) Observation: There are three IT staff members that are listed under the domain administrator group for the network. When signing onto a server, the staff use "administrator" as the login name. As a result there is no trail of who logged onto the server under "administrator".
   Recommendation: The District should create individual username and password accounts for those IT staff authorized to have server access. The user name "administrator" should be tagged so that anytime it is used an event or notification is sent. This would provide an audit trail for the District to monitor who is logging onto the server.
2) Observation: There are currently no advanced network security tests being performed on the firewall. The firewall and security may have some minor risk exposures that can easily be identified by performing vulnerability scans.
   Recommendation: We recommend the District consider contracting a third party company to run vulnerability scans or licensing vulnerability scanning software and perform periodic scans.

Network administration *(continued)*

3) Observation: Firmware updates are done on an annual basis. These updates should be performed more frequently to ensure the firmware is loaded with the most current patches. Recommendation: The District should perform updates to its firmware on a more regular basis.

Conclusion
The District has clearly placed significant thought and effort in the design and management of the network environment. It is secured and protected from unauthorized access. The network equipment is mostly modern, and components have been identified and planned to be replaced. There is a plan to modernize the server environment in the form of virtualization, which is ahead of schedule when compared to many school districts. Our review did not note any significant weaknesses. We feel the network is secure and operating effectively and efficiently.

Physical Inventory and Security

The District servers are located within the technology department. We noted that the door into the technology department is always locked and the door to the server room is also locked. The server room is protected from the elements and has no direct access from the outside of the building. There are 3 cooling systems in place to control the temperature of the room. The servers are stored in racks which are elevated from the floor. The servers are monitored 24 hours a day, 7 days a week by System Insight Manager. In the event of a malfunction the Network Administrator is notified.

District software and programs are network based. Each computer is given access to software specific for the needs of that department or user. Software licenses are tracked by the IT department through Helpstar. Most software licenses are licensed to the District based on FTE's. This has resulted in large savings for the District, because the District is only invoiced for what software is actually used. Unauthorized programs cannot be executed on any of the machines by any user other than the IT staff.

The District uses Microsoft Configuration Manager to monitor all Microsoft Windows updates as well as updates to application software such as Java, Adobe, and Flash. The IT department evaluates and test samples the product updates before installed globally. The District deploys McAfee antivirus software on all computers. Updates to engines and definitions are defined to be installed as soon as they are available and approved by the IT staff. Virus scans are configured to be performed on a regular basis. There is also real time virus protection.

Physical Inventory and Security *(continued)*

The District has a large scale of multi-function devices including computers, printers, Ipads, smartboards and projectors. The devices at each building are kept in locked rooms and are monitored. Spare devices and parts are inventoried and stored in a locked closet in the technology department. Ipads and laptops are assigned to faculty. Equipment costing over $500 is asset tagged and inventoried by the purchasing department. The District contracts IT Asset Management Group to periodically perform a detailed inventory count of equipment on hand. The District has not noted significant shrinkage of equipment. Most equipment have standard 3 year warranties. For certain equipment, the warranties are extended beyond the 3 years because it is inexpensive to do so. The District leases its computers then purchases them at the end of the term. The computer replacement cycle is 6 years. All old and damaged equipment has the hard drive cleaned before it is disposed.

Areas for potential improvement:

1) Observation: In the event of a server malfunction, the Network Administrator is immediately contacted. Although there has never been a setback with the current process, the District should consider including an additional administrator to be contacted in such an event.
   Recommendation: By assigning an additional administrator, the District would limit the dependency of one person being notified, in the event the Network Administrator was not reachable.
2) Observation: During our walk through of spare parts and equipment, we noted a significant amount of new computer monitors unopened and not used.
   Recommendation: The District is making an effort to limit the amount of monitors it receives in the future when purchasing new computers. The District should consider identifying old monitors amongst the locations and swapping them out with the new ones.

Conclusion

The District's equipment is mostly new and therefore running with the latest processors and loaded with the most current security programs. The equipment is kept in secured locations throughout the District and therefore difficult to move. When equipment is purchased it is tagged and tracked. IT parts are kept in a locked room and is inventoried. Parts are kept at a minimum to reduce the amount of inventory on hand. Disposed equipment are properly destroyed and the information is permanently erased from the hard drives.

Virtual Server Technology

The District has 15 physical servers and 22 virtual servers. The District will eventually phase out its physical servers and move to all virtual servers. There are many advantages in having virtual servers. Some of these advantages are as follows:

- High Availability – In the event of a failure, business operation can be immediately resume will little to no interruption.
- Scability – Allows the system to quickly accommodate a growing amount of work in a capable manner.
- Cost Savings – Due to its design, there is less need for hardware and software to accomplish the same setup.
- SANS Hardware – This setup allows the user to conduct snapshot backups, which provide for faster data and disaster recovery.

Areas for potential improvement:

1) Observation: The District does not utilize the Snapshot technology on its SAN.
   Recommendation: We recommend the District configure the Snapshot technology on its SAN to fully take advantage of the benefit of such equipment.

Virtual server technology is increasingly becoming mainstream because of its many advantages. The District is talking a proactive approach in implementing new and improving technology as it becomes feasible.

Disaster Recovery and Backups

The District has taken steps to ensure continuity of school operations in the event of an unforeseen IT failure. The District has adopted a written disaster recovery plan which provides the components to implement a disaster recovery operation. The District regularly tests parts of the disaster recovery plan to ensure its effectives. It should be noted that there is no backup or disaster recovery process that can absolutely mitigate the risk in the event of a failure. As experienced with the recent storms, while the IT staff reacted quickly, uncontrollable factors hindered the Seven Bridges School from being fully operational after the storm.

District backups are done each night using Backup Exec software. Each Friday night, a full backup is performed. Two months of backup tapes are kept in a fireproof safe. Backup tapes older than two months are sent to an offsite location. BOCES separately backs up the District's financial information from Finance Manager to a server farm where two weeks of backups are stored. In addition, the backups are transferred to tape stock and shipped to an additional offsite location.

The District has portable generators that can be used in the event of a power failure. The generators are capable to provide power enough to safely shut down the servers, but not enough to keep the technology fully operational. As part of its 3 year plan, the IT Department will evaluate the cost and benefit of installing a permanent generator.

Disaster Recovery and Backups *(continued)*

Areas for potential improvement:

1) Observation: The District periodically performs tests of its disaster recovery plan; however do not perform a full recovery scenario.
   Recommendation: We recommend the District identify critical systems and perform a full recovery of that system to ensure the disaster recovery is effective.

Conclusion
Over the past few years and more recently with Hurricane Sandy, the District has seen its share of devastating storms. Fortunately, the District survived through all with little disruption. We feel the disaster recovery plan in place is sufficient to have the District operational as quickly as possible. Our review came shortly after Hurricane Sandy had struck. We noted that the IT department acted quickly, exploring every option to bring Seven Bridges school back online. However, because of Con Edison restrictions the network provider was unable to restore their connection. We had also noted an immediate response from Lighttower during the aftermath. It is difficult to prepare for any disaster, however we feel the current disaster plan is sufficient.

Financial Information System Access

The financial information of the District is conducted through Finance Manager (FM). The program is widely used among other school districts. Finance Manager is supported by Southern Westchester BOCES. The IT Department does not have access to Finance Manager other than providing a user with viewing rights.

In order to access Finance Manager, the IT Department must first provide viewing rights to the program. Once an employee is given access to Finance Manager the District Treasurer will assign them specific user rights. The District Treasurer is the authorized Finance Manager administrator. Based on the employees' responsibilities the Treasurer will assign the appropriate rights. While we would normally suggest that users of the financial system should not be administering rights, the Business Office has implemented procedures to mitigate risk of unauthorized rights. On a quarterly basis the Assistant Superintendent for Business reviews the Finance Manager access rights and signs off that he has reviewed them. Each employee will create a personal password to Finance Manager which is required to be changed every 90 days.

Conclusion
There are good controls over the access files and user rights of Finance Manager. There is enough segregation to limit the ability for an unauthorized user from access. Finance Manager itself has controls built into the module that restrict users from certain tasks. The District also has procedures in place to prevent and/or detect misuse of Finance Manager. We tested the access rights of each employee within the Business Office to determine if they had the correct rights in Finance Manager based on position. All employees had proper access rights.

Internet Usage, Wireless Internet Connections and Remote Access

The District has established an internet use policy that all users must adhere to. Its wireless and remote access network is well controlled and protected. We did not note any significant weaknesses.

The District currently contracts with Lightspeed for filtering of accessible websites from District computers. The District also has the ability to add websites to the restricted list as it sees fit. This ensures that any new threats are eliminated immediately after they are discovered. Students and staff are restricted from the use of social networking sites such as Face Book, MySpace, and YouTube. These sites are restricted by the internet filtering software and therefore cannot be accessed by District computers. In addition to District computers, any other computers using the District's internet access would be subject to the same restrictions.

All employees and students must agree to the Acceptable Use Policy. This document can be found on the District's website. All new students also receive an entire District manual which they must read and have their parents sign. Once brought back to their building, the school office manager gives them access rights to the internet.

The District currently has wireless internet access points at the Education Center, Middle School, High School and certain areas of the Elementary School. The guest wireless network is open with limited internet access only. Students and faculty have the ability to use the guest wireless network or sign onto the District's network. To access the network the user requires individual log in information. The District's wireless network is integrated into an active directory and uses a SSL encryption for secure transmission of user ID's and passwords.

Faculty and administrators also have remote access to files and applications configured through a Citrix server. BOCES uses VPN for remote access for support on the Finance Manager and IEP Direct applications. The Citrix server provides the faculty with secured access to District applications, but does not allow them access to District computers. The IT staff specifically has remote desktop for network administration.

Areas for potential improvement:

1) Observation: A demilitarized zone (DMZ) was not established for the Citrix and Exchange servers.
   Recommendation: We recommend the District create a DMZ, for both servers and implement a SSL for its Citrix server.
2) Observation: Through the wireless connection, we were able to access chat rooms using our Windows based computer. Chat room access has been disabled for Mac and IOS machines only.
   Recommendation: The District should review its chat room policy and take the necessary steps in restricting chat room access for Window based computers.

Conclusion

The internet connectivity amongst the different locations is secure and redundant. Users are restricted from visiting unauthorized websites. We encourage the District to review its chat room access to ensure students cannot access chat rooms such as AOL AIM.

Email Accounts

The District provides faculty and administrators with district email addresses. The email is hosted through Microsoft Exchanger 2007. Students do not have email through the District's exchange server. The District is evaluating implementing Microsoft Office 365 to provide emails for students which will be hosted through Microsoft's cloud. All emails are filtered for spam, malware, and are scanned for viruses and phishing files.

The District has a dedicated email retention server which captures a backup of all incoming and outgoing email messages within the District. The emails are retained indefinitely. This retention server fulfills the Boards legal obligation for public information and FOIL requests. The District IT staff is the only District personnel with access to the data held on the retention server.

Areas for potential improvement:

1) Observation: The current Microsoft Exchange server is not fully patched to the latest service pack because of compatibility restrictions with Mimosa.
   Recommendation: The District should consider upgrading their Mimosa to one that supports a later version of Microsoft Exchange, and run the necessary service packs.

Conclusion
The email server is secure and the District's email retention policy is consistent with other school district policies. We did not note any significant weaknesses in this area.