Putnam Valley Central School District

Information Technology
Internal Audit Report
August 2017

August 30, 2017

Audit Committee
Putnam Valley Central School District
146 Peekskill Hollow Road
Putnam Valley, NY 10579

Dear Audit Committee members:

We have completed our internal audit of the Information Technology (IT) General Computer Control Environment of the Putnam Valley Central School District ("the District"). This area was recommended for audit in our FY16/17 risk assessment update report.

This internal audit report includes background information, the audit scope and objectives, a summary of audit procedures performed, a summary of audit findings and ratings, and our observations and recommendations.

The audit procedures performed included various tests, reviews, and evaluations in accordance with the *International Standards for the Professional Practice of Internal Auditing* promulgated by the Institute of Internal Auditors

We appreciate the fine level of cooperation provided to us by the District's staff during our audit and look forward to working with them in the future.

Very truly yours,

Accume Partners

Accume Partners

Tower 49, 12 East 49th Street
New York, NY 10017
p: 646.375.9500
f: 646.328.0011
accumepartners.com

Background

Accume Partners performed an IT General Computer Controls Review at the District. We reviewed the adequacy and effectiveness of controls supporting the computing environment and management oversight.

Audit Scope and Objectives

The purpose of the review was to evaluate and assess the adequacy of the procedures and controls in order to ensure that the District's computer systems are managed in a controlled manner. The procedures were performed in accordance with the District's Internal Audit Plan, which was reviewed and approved by management and the Audit Committee. Our work included the following areas:

- IT Strategy and Planning
- Outsourced Vendor Management
- Business Continuity Planning
- IT Infrastructure and Maintenance
- Information Security
- Systems Development and Maintenance
- System Operations
- IT Governance
- Critical Systems

Summary of Audit Procedures Performed

Our procedures included interviewing key personnel, reviewing policies and procedures, inspecting certain documents and reports, and testing the effectiveness of identified controls. We performed the following specific procedures:

- Reviewed management's oversight of the IT environment to determine if policies and procedures exist, are being followed, and are suitable for the IT environment.
- Reviewed the current Strategic Technology Plan and Technology Committee Meeting Minutes to identify the District's goals, action plans and the strategic planning process.
- Reviewed Board of Education Meeting Minutes to determine whether the Board is kept informed of information technology activities.
- Reviewed controls over third party vendors to determine if there was proper selection and oversight, and if adequate documentation was maintained to support vendor relationships.

- Reviewed vendor contracts and service level agreements for existence and compliance with terms.
- Reviewed network and application backup procedures for appropriateness and adequacy.
- Reviewed security administration procedures and user access reports for adequacy and appropriateness.
- Reviewed the District's IT Policies for completeness and adequacy.
- Reviewed the physical security environmental controls of the server room.
- Reviewed the Technology Organization Chart and IT job functions to determine whether such functions are appropriately segregated.
- Reviewed application security administration and password controls.
- Reviewed remote access (VPN) for appropriateness.
- Reviewed that only active employees, or authorized vendors and consultants of the District, had access to critical application systems, by comparing a listing of application level ID's to a listing of active and terminated employees provided by Human Resources.
- Reviewed application system password parameters for appropriateness.
- Reviewed the wireless LAN security parameters and encryption standards for adherence to best practices.
- Reviewed network monitoring controls and sample reports for existence.
- Reviewed the anti-virus software to determine whether it was operational and updated.
- Reviewed the Network Diagram to confirm the District's connectivity.
- Reviewed the Disaster Recovery and Business Continuity Planning procedures for appropriateness.
- Reviewed Disaster Recovery Test results for adequacy.
- Toured the Lower Hudson Regional Information Center (LHRIC) and reviewed the IT controls surrounding the processing that the LHRIC performs on behalf of the District.
- Reviewed the District's measures to address Cybersecurity.

Summary of Audit Findings and Ratings

As a result of the work performed, we noted the following observations that resulted in recommendations to improve internal controls and enhance operating policies and procedures. Detailed observations and recommendations follow this section.

Audit Area	Key Processes/Documents Reviewed	Recommendations	Rating
IT Strategy and Planning	• Instructional Technology Plan • Smart Schools Investment Plan • OSC IT Questionnaire • IT Organization Chart • IT Job Descriptions • Technology Committee Charter • Technology Committee Meeting Minutes • Board Of Education Meeting Minutes • Status of Current IT Projects and Planned IT Projects • Technology Budget • Equipment Insurance	None	Satisfactory
Outsourced Vendor Management	• Purchasing Policy and Procedures • LHRIC Service Level Agreement • LHRIC Installment Purchase Agreement • LHRIC IT Controls • LHRIC Service Organization Control 2 (SOC2) Report • Vendor Contracts (PowerSchool, Google For Education & CSI)	The District should monitor vendor Service Level Agreements (SLA's) to ensure that agreed upon services are being delivered. *(Observation #1)*	Satisfactory
Business Continuity	• Data Recovery and Disaster Plan • Business Operations Continuity and Disaster Preparedness Plan • LHRIC Finance Manager Disaster Recovery (DR) and Backup Procedures (nVision) • Finance Manager DR Test Results Memo (nVision)	None	Satisfactory

Audit Area	Key Processes/Documents Reviewed	Recommendations	Rating
IT Infrastructure and Maintenance	• Network Topology Diagrams • LHRIC Wide Area Network Security Procedures • LHRIC Data Center Controls & SOC2 Report • Hardware and Software Inventories • Hardware Disposal Procedures • Firewall Configuration and Event Monitoring Logs • Anti-Virus and Malware Monitoring • Wireless Security Controls • Intrusion Protection Procedures and Event Monitoring • LHRIC Internet Access Event Monitoring • CSI Remote Monitoring Agreement • Sample Monitoring Reports (Equipment, Network and Firewall) • Users with VPN Access	None	Satisfactory
Information Security	• Process for Enabling/Disabling Employee User Accounts • Employee Listings (Active, New Hires and Terminations) • Sample New Hire and Termination Approval Forms • User Access Listings (Finance Manager, PowerSchool, IEP Direct and VPN) • Application Password Parameters • Screen Inactivity Settings • Login Monitoring Reports • PVCSD and LHRIC Data Center Physical and Environmental Controls • Server Room Key Sign-in Logs	The District should perform a periodic user entitlement review of system access for all applications. *(Observation #2)*	Satisfactory
Systems Development and Maintenance	• Patch Management Process and Settings • Sample Patch Reports	None	Satisfactory

Audit Area	Key Processes/Documents Reviewed	Recommendations	Rating
System Operations	• LHRIC Remote Backup Service • Backup Process at Xand Co-location • Backup Log Snapshot • Helpdesk Reports/Logs • Sample Backup Restore	None	Satisfactory
IT Governance	• Student Use of District Technology Policy • Internet Safety Policy • Computer, Internet and E-mail Use Agreement • Laptop and Mobile Device Loan Agreement • Student Privacy Policy • Computer Resources and Data Management Policy • Information Security Breach and Notification Policy	The District should provide formal cybersecurity training to all system users on an annual basis. *(Observation #3)*	Satisfactory

Audit Ratings

Satisfactory	Indicates an acceptable system of internal control and satisfactory compliance with applicable policies, procedures and regulatory requirements. Findings indicate modest weaknesses that require management's attention.
Needs Improvement	Indicates weaknesses in the system of internal control and/or compliance with related policies, procedures and regulatory requirements. These findings require management's prompt resolution to prevent further deterioration and possible losses.
Unsatisfactory	Indicates significant weaknesses in the system of internal control and/or compliance with related policies, procedures and regulatory requirements. Management's immediate attention to these findings is required to prevent loss to the institution.

Observations and Recommendations

1. **Outsourced Vendor Management – Vendor Service Level Agreements (SLA's)**

   Observation: The District utilizes third party vendors to provide IT services including application support for the Student Information System (PowerSchool) and Network Monitoring (CSI). We noted that the PowerSchool SLA included Security Advisory Services and Quarterly Security Audits; however, there was no evidence that these services were provided to the District. In addition, the Network Assessment described in the CSI SLA has not been performed.

   School District Risk and/or Opportunity: The District's vendors may not be meeting the obligations of service level or contractual agreements.

   Recommendation: Review the current vendor SLA's and evaluate contractual vendor compliance with agreed upon terms and conditions.

   Management's Response: We agree with the observation and will review vendor SLA's for compliance.

   Proposed Implementation Date: Immediately.

   Responsible Party: Michael Lee

2. **Information Security – User Access Entitlement Review**

   Observation: A formal periodic review of user access entitlements is not performed. During our testing of application user access, we identified one former employee active in PowerSchool and several former employees with disabled accounts. It was determined that the former employee's account needed to remain active for a period of time. The password was changed to prevent unauthorized access from the original account holder. In addition, there were many users with IEP Direct system access who were not on the active employee list; however, upon further review, it was determined that these users were consultants who required access.

   School District Risk and/or Opportunity: Lack of a user access entitlement review could result in unauthorized system access.

   Recommendation: We recommend that the District perform a periodic review of system access rights for all applications to ensure that user ID's are for active employees or approved consultants and that rights align with job responsibilities. In addition, disabled accounts for former employees should be removed.

Management's Response: We agree with the observation and will develop a formal review process for system access rights.

Proposed Implementation Date: November 1, 2017

Responsible Party: Michael Lee

3. **Governance – Cybersecurity Awareness Training**

Observation: While we recognize that District staff are re-briefed on the Computer Use Agreements annually, formal cybersecurity awareness training has not been performed.

School District Risk and/or Opportunity: Lack of cybersecurity training and preparedness may result in loss of data and affect the confidentiality of non-public information.

Recommendation: With the continued risk of cybersecurity threats, we recommend that the District provide user awareness training for safe computing practices and response actions to all employees who have access to systems and data. Training should address the protection of non-public information and include information security basics as well as cybersecurity threats (i.e., Ransomware, Safe Web Browsing, Mobile Device Security, Phishing/Social Engineering, and Domain Spoofing).

Management's Response: We agree with the observation and will explore the best options for delivering cybersecurity training to all staff.

Proposed Implementation Date: 17-18 School Year

Responsible Party: Technology, Curriculum, and HR Departments.