accume partners

Hastings-on-Hudson Union Free School District

Information Technology Internal Audit Report May 2019

---

accume partners

May 23, 2019

Audit Committee
Hastings-on-Hudson Union Free School District
27 Farragut Avenue
Hastings-on-Hudson, NY 10706

Dear Audit Committee:

We have completed our internal audit of the Information Technology (IT) General Computer Control Environment of the Hastings-on-Hudson Union Free School District ("the District"). This area was recommended for audit in our FY18/19 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

12 East 49th Street, 5th Floor
New York, NY 10017
p: 646.375.9500
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
- Cybersecurity
- 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 District's IT Policies for completeness and adequacy.
- Reviewed the current Strategic Technology Plan to identify the District's goals, action plans and the strategic planning process.
- Reviewed the District Organization Chart and IT job functions to determine whether such functions are appropriately segregated.
- 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 the backup restore process and sample file restores.
- Reviewed the System Support/Help Desk process and sample incident reporting.
- Reviewed security administration procedures and user access documentation for adequacy and appropriateness.
- Reviewed the physical security and environmental controls of the server room.
- Reviewed remote access (VPN) for appropriateness.
- Reviewed Network Administrative accounts for appropriateness.
- Reviewed that only active employees or authorized vendors and consultants of the District had access to critical application systems and the network by comparing a listing of network and application level user ID's to a listing of active and terminated employees provided by Human Resources.
- Reviewed Acceptable Use Polices for a sample of new hires to determine whether they were signed prior to providing network access.
- Reviewed network and application system password parameters for appropriateness.
- Reviewed the wireless LAN security parameters and encryption standards for adherence to best practices.
- Reviewed network and internet monitoring controls and sample reports for existence.
- Reviewed vulnerability assessment reports to determine whether the District addresses potential vulnerabilities.
- Reviewed Patch Management reports to determine whether patches are up to date.
- Reviewed the application change control process to determine whether application upgrades are documented and communicated to the District.
- Reviewed firewall monitoring and the firewall change control process.
- Reviewed the anti-virus software to determine whether it was operational and updated.

- Reviewed the Network Diagram to confirm the District's connectivity.
- Reviewed hardware and software inventories for existence.
- Reviewed the Disaster Recovery and Business Continuity Planning procedures for appropriateness.
- Reviewed Disaster Recovery Test results for adequacy.
- Reviewed the District's insurance policies to determine whether equipment and cybersecurity coverage is included.
- Reviewed security awareness training to determine whether the District provides cybersecurity awareness training to staff.
- 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 LHRIC's SOC 2 Report (Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy) and tests of operating effectiveness.
- Reviewed the District's measures to address Cybersecurity.
- Followed up on previous audit observations to ensure that recommendations were implemented.

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 • District Organization Chart • LHRIC Field Support Service Level Agreement • Technology Meeting Notes • Board of Education Meeting Minutes • Status of Current IT Projects and Planned IT Projects • LHRIC Request for Services - Technology Budget • Equipment Insurance • Cyber Insurance	None	Satisfactory
Outsourced Vendor Management	• List of Key IT Service Providers • Purchasing and Bidding Policies and Procedures • New Vendor Request Form • LHRIC Field Support Service Level Agreement • LHRIC Financial Services Service Level Description • LHRIC Request for Services • LHRIC IT Controls • LHRIC Service Organization Control 2 (SOC2) Report	The District's Purchasing Policies should include a Contracting for Professional Services Policy. *(Observation #1)*	Needs Improvement
Business Continuity	• LHRIC Financial Services SLA • LHRIC Finance Manager DR Services • Business Operations Continuity and Disaster Preparedness and Activation Plan • Finance Manager Backup and Security Procedures • Results of Disaster Recovery Testing (nVision)	The District's Disaster Recovery Plan should be formalized, documented and include all critical processes and services. *(Observation #2)*	Satisfactory

Audit Area	Key Processes/Documents Reviewed	Recommendations	Rating
IT Infrastructure and Maintenance	• District Technology Profile • Network Topology Diagrams • LHRIC Wide Area Network Security Procedures • LHRIC Data Center Controls & SOC2 Report • Hardware and Software Inventories • Hardware Disposal Procedures • Sample eWaste Certificate of Recycling • Firewall Configuration and Event Monitoring Logs • Anti-Virus and Malware Settings and Monitoring • Wireless Security Controls • LHRIC Intrusion Protection/Detection Procedures and Event Monitoring • LHRIC Internet Access Event Monitoring • Sample Server and Capacity Monitoring Reports • Users with remote VPN Access • Domain Admin Users • Firewall Change Control Process • Qualys Vulnerability Assessment Report	In order to detect security vulnerabilities and the patches needed to fix them, we recommend regular vulnerability assessments. *(Observation #3)* The District should ensure that procedures are in place to track and reconcile portable devices. *(Observation #4)* The District should periodically monitor employee Internet Activity to ensure compliance with Acceptable Use Policies. *(Observation #5)*	Needs Improvement
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 (Network, nVision, eSchoolData, IEP Direct, Horizon and VPN) • Audit Trail of nVision Access Changes • Network and Application Level Password Parameters • Hastings and LHRIC Data Center Physical Security and Environmental Controls	The District should disable/delete former employee user accounts and perform a periodic user entitlement review of system access for the network and all applications. In addition, Network Access Revocation Forms should be completed for all terminated employees. *(Observation #6)*	Needs Improvement

Audit Area	Key Processes/Documents Reviewed	Recommendations	Rating
		Password expiration intervals and complexity should be enabled within the eSchoolData student information system. *(Observation #7)*	
Systems Development and Maintenance	• Patch Management Process and Settings • Sample Patch Reports • Audit Trail of nVision Database Changes • nVision Release Upgrade Process • eSchoolData Release Upgrade Process	None	Satisfactory
System Operations	• LHRIC Remote Backup Service • Backup Retention Policy • Backup Schedules • Sample Backup Reports and Daily Emails • Sample Backup Restores • Service Now Helpdesk Reports/Logs	None	Satisfactory
IT Governance	• Computer Resources and Data Management Policy • Information Security Breach and Notification Policy • Internet Safety Policy • Code of Conduct Policy • Student Use of Privately Owned Technology Policy • Acceptable Technology Use Policies • Disposal of District Property Policy • Responsible Use Policy Training and Compliance • LHRIC Data Privacy Notice	The District should provide formal cybersecurity training to all system users on an annual basis. *(Observation #8)* The District should ensure that all staff members acknowledge that they have read and understand the Acceptable Technology Use Policies prior to obtaining system access. *(Observation #9)*	Needs Improvement

Audit Area	Key Processes/Documents Reviewed	Recommendations	Rating
		The District should ensure that regulations and procedures have been documented to support the IT Policies. *(Observation #10)*	

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 – Contracting for Professional Services Policy

Observation: The District's Purchasing Policies do not include provisions for Contracting for Professional Services as required by General Municipal and Education Law. There is a policy reference in the Purchasing Policy to guidance on purchasing professional services; however, this policy does not exist.

School District Risk and/or Opportunity: The absence of a Contracting for Professional Services Policy may result in inadequate vendor due diligence as well as non-compliance with legally required policies.

Recommendation: The District should formally adopt a Contracting for Professional Services Policy.

Management's Response:
The finance office has already made the policy committee aware of the need to revise this policy.

Proposed Implementation Date:
2019-2020 school year

Responsible Party:
Policy Committee

2. Business Continuity Planning – Plan Documentation

Observation: Although the District has a documented Disaster Recovery Plan for Finance Manager (nVision) that is tested on an annual basis with the LHRIC, plans and procedures for the recovery of other critical processes have not been documented.

School District Risk and/or Opportunity: The absence of documented Disaster Recovery procedures for all critical functions could impact the timely restoration of operations.

Recommendation: The District should have a formal documented Disaster Recovery Plan that includes action plans for all critical functions. The recovery strategy should document:

- Roles and responsibilities of key personnel

- Critical processes and services prioritized based on business impact
- Procedures for employees (i.e., communication methods, alternate work locations)
- Communication protocols with outside parties such as law enforcement and IT vendors
- Technical details concerning how systems and data will be restored and resource requirements
- Alternate methods for accessing critical systems
- Backup methods and storage policies and procedures
- Periodic testing of the plan

Management's Response:
The District Technology Team will work with Building level Administration and the LHRIC to develop a disaster recovery plan for critical systems outside of the financial system (nVision).

Proposed Implementation Date:
2019-2020 school year

Responsible Party:
District Technology Team

3. IT Infrastructure and Maintenance – Vulnerability Assessments

Observation: Although a Qualys vulnerability scan was run in response to our audit request, regularly scheduled vulnerability assessments of network devices do not occur.

School District Risk and/or Opportunity: Scanning the network and systems on a regular basis will minimize the time of exposure of known vulnerabilities.

Recommendation: In order to detect security vulnerabilities and the patches needed to fix them on a timely basis, we recommend establishing a formal schedule of vulnerability assessments. The results of the assessments should be evaluated and a remediation plan should be documented for identified vulnerabilities based on criticality.

Management's Response:
The district networking team is presently working with the LHRIC to establish a schedule results based action plan for district vulnerability assessments. Preliminary discussions have been around a twice a year schedule. Deeper discussions are needed for interpretation and reporting lines to the district. We expect initial implementation during the 19-20 school year.

Proposed Implementation Date:
2019-2020 school year

Responsible Party:
District networking team working with the LHRIC.

4. IT Infrastructure and Maintenance – Portable Device Inventories

Observation: An annual end user device inventory is performed over the summer; however, with the frequent use of shared portable devices (i.e., Chromebooks) in the middle and elementary schools, accountability for the devices should be more frequent.

School District Risk and/or Opportunity: Unaccounted for devices may result in financial loss to the District.

Recommendation: The District should establish procedures to track and reconcile portable devices on a periodic basis to ensure that all devices are accounted for.

Management's Response:
The high school has deployed mobile devices (Chromebooks) via a one-to-one model, and Hillside elementary school has their chromebook carts assigned by room. Farragut middle schools has been, up to now in a hybrid model of some chromebooks carts dedicated to rooms, and others shared by section, where the carts reside in hallways. Beginning with the 19-20 school year, the district is phasing out the shared model, and moving to dedicating/assigning devices to classrooms.

Proposed Implementation Date:
2019-2020 school year

Responsible Party:
District technology team working with Building level Administration.

5. IT Infrastructure and Maintenance – Internet Activity Monitoring

Observation: Although the Board has adopted an Acceptable Use Policy and web filters are in place, monitoring Internet activity for inappropriate use does not occur on a routine basis.

School District Risk and/or Opportunity: Lack of adequate oversight of Internet usage may result in undetected policy violations.

Recommendation: The District should establish a standard schedule to monitor employee Internet Activity usage through available LHRIC Lightspeed reports to detect unacceptable use.

Management's Response:
The district technology team is presently working with the LHRIC systems and operations team to produce an aggregate scheduled report solution for the district that can provide a profile and insight into the district's Internet browsing activity. We expect to have a solution in place for the 19-20 school year.

Proposed Implementation Date:
2019-2020 school year

Responsible Party:
The district technology team is presently working with the LHRIC systems and operations team.

6. Information Security – Security Administration

Observation: IT does not always receive notification of employee terminations which has resulted in user access not being disabled in a timely manner. While the process for access removal is to submit the request via the Service Now help desk with a Network Revocation Form, our testing of network and application user access found that several users did not have the appropriate forms and a help desk request was not initiated. We also identified many former employees enabled in Active Directory and IEP Direct (no exceptions were noted in nVision, eSchoolData or Horizon). In addition, a formal periodic review of user access entitlements is not performed.

School District Risk and/or Opportunity: User accounts that are not removed or disabled in a timely manner could result in unauthorized system access.

Recommendation: We recommend that the District immediately disable/delete accounts for former employees and implement procedures to ensure that employee exit notifications occur on a timely basis with appropriate documentation. In addition, the District should perform a periodic review of system access rights for the network and all applications to ensure that user ID's are for active employees or approved consultants and that rights align with job responsibilities.

Management's Response:
Business Office/HR department will make sure that timely notification of changes in employee status be quickly and consistently made to the IT department.

Proposed Implementation Date:
2019-2020 school year

Responsible Party:
Business Office and HR department.

7. Information Security – Password Expiration and Complexity Parameters

Observation: Passwords are not set to expire within the eSchoolData student information system. In addition, complexity is not a requirement for eSchoolData passwords.

School District Risk and/or Opportunity: Inadequate password controls may result in a user's account being compromised.

Recommendation: Password expiration intervals and complexity should be enabled within the eSchoolData student information system.

Management's Response:
The District will begin to require password expiration intervals to be set in eSchoolData. An enhancement request has already been submitted by the LHRIC to have password complexity requirements added to the eSchoolData software.

Proposed Implementation Date:
2019-2020 school year

Responsible Party:
District eSchoolData security Administrators and the LHRIC.

8. Governance – Cybersecurity Awareness Training

Observation: While we recognize that periodic email reminders are sent to staff with regard to email security, 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:
The district technology team is working with the LHRIC to provide a staff development solution specific to cybersecurity awareness. One specific facet of this training will focus on email security. We expect to have a solution in place for the 19-20 school year.

Proposed Implementation Date:
2019-2020 school year

Responsible Party:
District networking team working with the LHRIC.

9. Governance – Acceptable Technology Use Policy Acknowledgements

Observation: During our testing of policy acknowledgements, we were unable to obtain signed documentation for one new hire.

School District Risk and/or Opportunity: Acknowledging understanding of policies ensures staff are aware of their responsibilities.

Recommendation: The District should implement procedures to ensure that all staff members acknowledge that they have read and understand the Acceptable Technology Use Policies prior to obtaining system access.

Management's Response:
This was one oversight but we will continue to ensure we tighten up our HR practices to make sure all staff are compliant.

Proposed Implementation Date:
Immediately

Responsible Party:
Business Office/HR

10. Governance – Policy Regulations

Observation: While the District has adopted an Information Security Breach and Notification Policy and a Computer Resources and Data Management Policy, regulations and procedures have not been documented to address the policies.

School District Risk and/or Opportunity: Documented regulations can help improve accountability and ensure that internal controls are identified, operational and effective. The procedures can also assist with continuity of business operations during times of change and turnover.

Recommendation: The District should ensure that regulations and procedures have been documented to support the IT Policies.

Management's Response:
We agree with this recommendation and will work with the New Superintendent and board's policy committee to create procedures.

Proposed Implementation Date:
2019-2020 school year

Responsible Party:
Business Office/Central Office/BOE