Cherry Bekaert
Your Guide Forward

Hastings-on-Hudson
Union Free School District

Information Technology
Internal Audit Report
November 2023

November 20, 2023

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 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.

Sincerely,

Cherry Bekaert Advisory LLC

Cherry Bekaert Advisory LLC

Background

We 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 where the information was provided:

- 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 IDs 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	• Internal Audit Risk Assessment • Internal Audit Reports • 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	The IT audit risk assessments should be finalized. *(Observation #1)* Internal IT audit report findings should be acted upon. *(Observation #2)* The District should develop a Technology Committee charter that notes the written responsibilities for the committee. *(Observation #3)* The Technology Committee meetings should be documented. *(Observation #4)* Ensure that insurance policies are current and adequately cover IT related equipment. *(Observation #5)*	Needs Improvement
Outsourced Vendor Management	• List of Key IT Service Providers • Purchasing and Bidding Policies and Procedures • New Vendor Request Form	None	Satisfactory

Audit Area	Key Processes/Documents Reviewed	Recommendations	Rating
	• 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		
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, services, and roles and responsibilities. *(Observation #6)* Ensure that Disaster Recovery testing for all critical systems and processes is performed on an annual basis. *(Observation #7)* Ensure that Disaster Recovery testing for all critical systems and processes is reported to the Board on an annual basis. *(Observation #8)*	Needs Improvement
IT Infrastructure and Maintenance	• District Technology Profile • Network Topology Diagrams • LHRIC Wide Area Network Security Procedures • LHRIC Data Center Controls & SOC2 Report	Regular internal vulnerability assessments should be performed. *(Observation #9)*	Needs Improvement

Audit Area	Key Processes/Documents Reviewed	Recommendations	Rating
	• 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	Regular external penetration assessments should be performed, documented, and any issues discovered resolved. *(Observation #10)* *Wireless network policy and procedures should be developed. (Observation #11)*	
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, 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 review system access for Active Directory. Ten accounts were observed in the Active Directory listing but were not on the employee list and were not identified as to be on the system through inquiry with management. *(Observation #12)* The District should disable/delete former employee user accounts and perform a periodic user entitlement	Unsatisfactory

Audit Area	Key Processes/Documents Reviewed	Recommendations	Rating
		review of system access for Active Directory. 47 terminated users were observed on the system. *(Observation #13)* The District should disable/delete former employee user accounts and perform a periodic user entitlement review of system access for eSchoolData. Four terminated users were observed on the system: *(Observation #14)* The District should disable/delete former employee user accounts and perform a periodic user entitlement review of system access for IEP Direct. Ten terminated users were observed in the IEP Direct system. *(Observation #15)* The District should ensure the Service Now (SNOW) Tickets are completed for all terminated employees. *(Observation #16)*	

Audit Area	Key Processes/Documents Reviewed	Recommendations	Rating
		The District should ensure the Service Now (SNOW) Tickets are completed for all new employees. *(Observation #17)* Password expiration intervals and complexity should be enabled within the eSchoolData student information system. *(Observation #18)* Password length should be increased to a minimum of eight characters for the nVision system. *(Observation #19)*	
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

Audit Area	Key Processes/Documents Reviewed	Recommendations	Rating
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 awareness training to all system users on an annual basis. *(Observation #20)* Ensure that an IT/GLBA risk assessment is conducted. *(Observation #21)*	Needs Improvement

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. IT Audit Risk Assessment

Observation: The District's IT Audit Risk Assessment was provided in a draft form dated April 2022 and no final assessment had been issued or approved for the audit period.

School District Risk and/or Opportunity: The absence of a final approved assessment may result in inadequate audit coverage.

Recommendation: The District should formally approve IT audit risk assessments within a reasonable timeframe of receiving a draft report.

Management's Response: Management will work with Cherry Bekaert to ensure that on a go forward basis, the IT Audit Risk Assessment is finalized.

Proposed Implementation Date: 3/31/2024

Responsible Party: Maureen Caraballo, Business Official and Nick Macri, Deputy Treasurer

2. Internal IT Audit Reports

Observation: Internal IT audit reports should be acted upon. All items from the previous Audit Report were not completed or had no response from management.

School District Risk and/or Opportunity: The lack of audit item remediation and tracking or at a minimum of management responses can lead to un-remediated IT security issues.

Recommendation: The District should formally approve IT audit risk assessments within a reasonable timeframe of receiving a draft report.

Management's Response: Management will work with Cherry Bekaert to determine which items in which IT Audit reports are still open, and ensure that those items are addressed. Per discussion with Cherry Bekaert, there are items in the 2019 IT Audit report for The Hastings on the Hudson School District that may still be open.

Proposed Implementation Date: 3/31/2024

Responsible Party: Maureen Caraballo, Business Official and Nick Macri, Deputy Treasurer

3. District Technology Committee Charter

Observation: The Districts Technology Committee charter was not provided for review.

School District Risk and/or Opportunity: The lack of a Technology Committee charter can lead to uncertainty and lack of follow-up responsibilities from Technology Committee meetings.

Recommendation: The District should ensure that a Technology Committee charter that notes the written responsibilities for the committee is in place.

Management's Response: Management will work with Cherry Bekaert to develop a Technology Committee Charter that will be used on a go forward basis. Governance of The Technology Committee can be established by the Board and should include at least one Board member, but can also include key Technology employees of the School District.

Proposed Implementation Date: 3/31/2024

Responsible Party: Maureen Caraballo, Business Official and Nick Macri, Deputy Treasurer

4. District Technology Committee Meeting Minutes

Observation: The Technology Committee minutes were not provided for review.

School District Risk and/or Opportunity: The lack of Technology Committee minutes can result in items not being followed-up for resolution.

Recommendation: The District should ensure the Technology Committee meetings are documented.

Management's Response: Management will work with Cherry Bekaert to develop a Technology Committee Charter that will be used on a go forward basis. Governance of The Technology Committee can be established by the Board and should include at least one Board member, but can also include key Technology employees of the School District. Meeting minutes will be developed as the Technology Committee meets and records minutes.

Proposed Implementation Date: 3/31/2024

Responsible Party: Maureen Caraballo, Business Official and Nick Macri, Deputy Treasurer

5. IT related Insurance Policy

Observation: The IT related insurance policies were not provided for review.

School District Risk and/or Opportunity: The lack of adequate IT insurance coverage can result in unexpected expenses.

Recommendation: Ensure that insurance policies are current and adequately cover IT related equipment.

Management's Response: Management will have available and provide documentation to substantiate the IT insurance policy or policies that may be in place.

Proposed Implementation Date: 3/31/2024

Responsible Party: Maureen Caraballo, Business Official and Nick Macri, Deputy Treasurer

6. Business Continuity Planning – Plan Documentation

Observation: Although the District has a documented Disaster Recovery Plan for 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: Management concurs with Internal Audit's recommendation and will implement accordingly.

Proposed Implementation Date*:* 3/31/2024

Responsible Party*:* Melissa Szymanski, Assistant Superintendent and Maureen Caraballo, Business Official

7. Disaster Recovery Testing

Observation: Disaster Recovery testing evidence for all critical systems and processes was not provided for review. Only testing for nVision was provided.

School District Risk and/or Opportunity: The lack of adequate IT related Disaster Recovery testing can lead to delays and unexpected results if a real event occurs.

Recommendation: Ensure that Disaster Recovery testing for all critical systems and processes is performed on an annual basis.

Management's Response: Management concurs with Internal Audit's recommendation and will implement accordingly.

Proposed Implementation Date: 3/31/2024

Responsible Party: Melissa Szymanski, Assistant Superintendent and Maureen Caraballo, Business Official

8. Disaster Recovery Testing Reporting

Observation: Reports for Disaster Recovery testing reports to the Board were not provided for review.

School District Risk and/or Opportunity: The lack of adequate IT related Disaster Recovery testing reports to the Board can lead to lack of confidence from the Board in the IT recovery and redundancy solutions.

Recommendation: Ensure that Disaster Recovery testing for all critical systems and processes is performed on an annual basis.

Management's Response: Management concurs with Internal Audit's recommendation and will implement accordingly.

Proposed Implementation Date: 12/31/2023

Responsible Party: Melissa Szymanski, Assistant Superintendent and Maureen Caraballo, Business Official

9. Internal Vulnerability Assessments

Observation: Evidence of internal vulnerability assessments of the network was not provided for review.

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

Recommendation: Regular internal vulnerability assessments should be performed, documented and any issues discovered resolved.

Management's Response: Management concurs with Internal Audit's recommendation and will work with LHRIC to implement the recommendation accordingly.

Proposed Implementation Date*:* 3/31/2024

Responsible Party*:* Jean Benitez, Account Manager and Maureen Caraballo, Business Official

10. External Penetration Assessments

Observation: Evidence of external penetration assessments of the network was not provided for review.

School District Risk and/or Opportunity: Penetration testing the external network and systems on a regular basis can minimize the time of exposure of known vulnerabilities.

Recommendation: Regular external penetration assessments should be performed, documented and any issues discovered resolved.

Management's Response: Management concurs with Internal Audit's recommendation and will work with LHRIC to implement the recommendation accordingly.

Proposed Implementation Date*:* 3/31/2024

Responsible Party*:* Jean Benitez, Account Manager and Maureen Caraballo, Business Official

11. IT related Wireless Policy

Observation: Wireless network policy and procedures were not provided for review.

School District Risk and/or Opportunity: The lack of adequate wireless networking documentation can lead to a lack of controls and security gaps for the overall network.

Recommendation: Wireless network policy and procedures should be developed.

Management's Response: Management concurs with Internal Audit's recommendation and will implement accordingly.

Proposed Implementation Date: 3/31/2024

Responsible Party: Jean Benitez, Account Manager and Maureen Caraballo, Business Official

12. Undocumented Users in Active Directory

Observation: Ten accounts were observed in the Active Directory listing but were not on the employee list and were not identified as acceptable to be on the system through inquiry.

School District Risk and/or Opportunity: Unauthorized network users can lead to security issues or the loss of confidential information.

Recommendation: The District should review system access for Active Directory especially for the following ten users that were not identified during the audit.

Management's Response: Management concurs with Internal Audit's recommendation and will implement accordingly.

Proposed Implementation Date: 3/31/2024

Responsible Party: Jean Benitez, Account Manager and Maureen Caraballo, Business Official

13. Terminated Users in Active Directory

Observation: Forty-seven (47) terminated user accounts were observed in the Active Directory listing.

School District Risk and/or Opportunity: Unauthorized network users can lead to security issues and the loss of confidential information.

Recommendation: The District should review accounts for Active Directory especially for the following forty-seven terminated users that were observed during the audit. The District should also review access logs to ensure that the accounts have not been accessed since termination.

Management's Response: Management will work with Cherry Bekaert to validate and determine the accuracy of the terminated employees, and make sure that terminated employees are removed from Active Directory.

Proposed Implementation Date: 3/31/2024

Responsible Party: Jean Benitez, Account Manager and Maureen Caraballo, Business Official

14. Terminated Users in eSchoolData system

Observation: Three (3) terminated user accounts were observed in the eSchoolData listing.

School District Risk and/or Opportunity: Unauthorized users can lead to security issues and the loss of confidential information.

Recommendation: The District should review accounts in eSchoolData especially for the following four terminated users that were observed during the audit. The District should also review access logs to ensure that the accounts have not been accessed since termination.

Management's Response: Management will work with Cherry Bekaert to validate and determine the accuracy of the terminated employees, and make sure that terminated employees are removed from the eSchoolData system.

Proposed Implementation Date: 3/31/2024

Responsible Party: Melissa Szymanski, Assistant Superintendent and Maureen Caraballo, Business Official

15. Terminated Users in IEP system

Observation: Eight (8) terminated user accounts were observed in the IEP system listing.

School District Risk and/or Opportunity: Unauthorized users can lead to security issues and the loss of confidential information.

Recommendation: The District should review accounts in IEP especially for the following four terminated users that were observed during the audit. The District should also review access logs to ensure that the accounts have not been accessed since termination.

Management's Response: Management will work with Cherry Bekaert to validate and determine the accuracy of the terminated employees, and make sure that terminated employees are removed from the IEP system.

Proposed Implementation Date: 3/31/2024

Responsible Party: Laura Sullivan, Director of Special Education and Maureen Caraballo, Business Official

16. Lack of Service Now Tickets for terminated employees

Observation: IT does not always receive notification of employee terminations via Service Now (SNOW) tickets, which has resulted in user access not being disabled in a timely manner as noted in the observations above. Only four of a sample of 25 terminated users had SNOW tickets.

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: The District should immediately submit Service Now tickets for terminated employees.

Management's Response: Management concurs with Internal Audit's recommendation and will implement accordingly.

Proposed Implementation Date*:* 3/31/2024

Responsible Party*:* Lynn Walker, Personnel Assistant and Maureen Caraballo, Business Official

17. Lack of Service Now Tickets for new employees

Observation: IT does not always receive notification of new employees via Service Now (SNOW) tickets, which has resulted in user access not being recorded and AUP forms note being completed. Only four of a sample of 25 new users had SNOW tickets with a signed AUP included.

School District Risk and/or Opportunity: User accounts that are not documented could result in unauthorized system access as well as unsinged AUPs.

Recommendation: The District should submit Service Now tickets for all new employees. Additionally, the District should ensure all employees have a signed AUP on file starting with four (4) from the sample reviewed: POZO SCHMIDT FRANCISCO, ORTIZ, CHARLES M, NORTON, JUDITH A, and ANTASH, GREGORY R.

Management's Response: Management concurs with Internal Audit's recommendation and will implement accordingly.

Proposed Implementation Date*:* 3/31/2024

Responsible Party*:* Lynn Walker, Personnel Assistant and Maureen Caraballo, Business Official

18. Lack of Password Expiration and Complexity Parameters for eSchoolData

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: Management concurs with Internal Audit's recommendation and will implement accordingly.

Proposed Implementation Date*:* 3/31/2024

Responsible Party*:* Melissa Szymanski, Assistant Superintendent and Maureen Caraballo, Business Official

19. Insufficient Password Length for nVision

Observation: Passwords length for the nVision system is set to seven (7) and should be minimum of eight (8).

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

Recommendation: Password length should be increased to a minimum of eight characters for the nVision system. Password expiration intervals and complexity should be enabled within the eSchoolData student information system.

Management's Response: Management concurs with Internal Audit's recommendation and will implement accordingly. Management will work with the external provider to determine if the recommended password length can be implemented and will move forward accordingly.

Proposed Implementation Date*:* 3/31/2024

Responsible Party*:* Jean Benitez, Account Manager and Maureen Caraballo, Business Official

20. Cybersecurity Awareness Training

Observation: Cybersecurity awareness training has not been proved to all users. A sample of the employee listing versus the training records indicated that only 239 of the 392 sampled had training on file.

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: The District should provide formal cybersecurity awareness training to all system users on an annual basis.

Management's Response: Management will work with personnel at the school district to determine a threshold for compliance and within the determined threshold for compliance. Management will work to ensure that employees are compliant with cybersecurity training requirements.

Proposed Implementation Date: 3/31/2024

Responsible Party: Lynn Walker, Personnel Assistant and Maureen Caraballo, Business Official