PREPARING STUDENTS FOR LIFE

Through Academic Achievement · Personal Well-Being · Career Readiness

July 13 **2020**

REPORT OF THE AUDIT COMMITTEE

The Audit Committee met on Wednesday, June 24, 2020 at 4:30 PM via the BlueJeans Video Conferencing Tool.

VIRTUAL ATTENDEES

Audit Committee Members

Chatika Britton, Jennifer Couser, Jim Crosset, Christine Fisher, David Foote, Elizabeth Gutridge, Thomas D. Heldman, Daniel E. Holthaus, Carol Lawrence, Clarice Warner

Administration

Laura Mitchell, Superintendent; Kevin Ashley, Director of Financial Reporting; Jeremy Gollihue, Chief Information Officer; Isaac Karn, Internal Audit Staff; Lauren Roberts, Director of Internal Audit; Brian Switalski, ITM Manager Information Security; Jennifer Wagner, CFO/Treasurer

Finance Committee

Eve Bolton, Finance Committee Chair; Melanie Bates; Ben Lindy

Financial Updates

Future of Schools

Superintendent Mitchell updated the Committee on her Future of Schools Plan.

She informed the group about the following three key messages that are a major focus of the Plan.

Key messages

1. Safety and Health of Students and Staff
2. Academic Acceleration
3. Equity

She also educated the Committee about the following areas outlined in her Plan.

- Review of the Center for Disease and Control Prevention Considerations for Schools
- Academic/Safety Risks
- Comparison of Five Models for Blended Learning
- Highlight of how other local communities are opening their schools

Treasurer Wagner informed the group about the financial implications due to COVID-19 and about the financial impact around opening and managing schools in a new way. She also discussed with the Committee various costs for the five models for Blended Learning.

Daniel Holthaus inquired as to how the Audit Committee could assist in opening of the schools. Finance Committee Chair Bolton advised that assistance is needed for access to Information Technology equipment, sustaining current dollars and building cash reserves and commitments to communities to have access.

Network Security Assessment Results Presentation

Brian Switalski, ITM Manager Information Security, introduced Keyan Shod of JW Affinity - IT Premier Solutions Provider. The Network Security Assessment was completed during the execution of the Fiscal Year 2020 Internal Audit Plan, but the presentation was postponed due to the impacts of COVID-19 on the Audit Committee meeting schedule.

Mr. Shod updated the group on his work in the following areas: (1) Assessment Scope, (2) Key Findings, (3) Detailed Findings and Recommendations, and (4) Summary.

The Scope: The IT Security Profile Assessment Project is intended to provide CPS a clear understanding of the environment's current Information Security posture as well as recommendations to enable CPS to implement a robust Information Security Program Office

The Main Objectives of the assessment were to:

1. Perform and audit of security processes and policies in defined technical engagement areas.
2. Performing vulnerability testing of defined technical engagement areas.
3. Create IT Security Training Content and deliver via onsite training and computer-based training.
4. Consolidate and provide assessment findings and provide recommendations for remediation.

The Goals of the assessment were to:

1. Provide data, analyses, and reports to establish an initial Security Profile for CPS.
2. Identify any existing vulnerabilities and recommend remediation.
3. Provide future state recommendations for establishing a robust Information Security Program.
4. Develop and deliver focused IT Security Training content.

Assessment Findings and CPS Response:

IT Security Policy

Risk	Key Findings	Impact	Recommendation	CPS Status	CPS Response
	CPS lacks a process to effectively evaluate and communicate information security risks to leadership.	IT cannot effectively communicate how risks impact CPS' broader business objectives, translate risk metrics and details into language of business leaders.	Implement a Certification and Accreditation process for risk management in order to properly evaluate, test and further examine security controls of an information system.	Planning Phase	Information Security will work with the appropriate stakeholders. Target dated dependent on prioritization.
	CPS Lacks effective security incident response.	CPS will not be able to efficiently detect, respond to, and recover from security incidents.	Implement a comprehensive security incident response capability program based on NIST Standards.	Complete	A formalized and documented Incident Response Plan (IRP) has been completed and team meetings are scheduled for July 1 for kick off.
	CPS lacks a disaster recovery plan for critical applications.	CPS is currently unable to effectively determine expected downtime for applications and proper allocation of resources in order to restore service.	Develop a disaster recovery plan for business-critical applications using NIST guidelines.	Complete	A formalized and documented Disaster Recovery Plan (DRP) has been created. Cooperation between ITM and InfoSec to increase our recoverability will continue.

External Network Vulnerability

Risk	Key Findings	Impact	Recommendation	CPS Status	CPS Response
	CPS lacks a vulnerability management process for applications, services, and systems.	Absent this process, CPS cannot continuously monitor vulnerabilities and the associated risk.	Implement a comprehensive Vulnerability Management and Risk Mitigation Strategy.	Planning Phase	Information Security will work with the appropriate stakeholders. Target date dependent on prioritization.
	No firewall policy exists.	CPS administrators have no official documentation to refer to when determining appropriate traffic types or auditing firewall policies.	Develop a firewall policy utilizing NIST guidelines to guide implementation and administration of of CPS firewalls.	Planning Phase	Information Security will work with the appropriate stakeholders. Target date dependent on prioritization.

Internal Network Vulnerability

Risk	Key Findings	Impact	Recommendation	CPS Status	CPS Response
	Ineffective patch management of 3rd party applications.	CPS computers with these applications are vulnerable to compromise to due outdated software versions.	Establish a patch management solution that will inventory, patch, and verify patch levels of 3rd party applications.	Planning Phase	Information Security will work with the appropriate stakeholders. Target dated dependent on prioritization.
	Outdated and unsupported OS and applications exist in the environment.	These systems are in a vulnerable state and security vulnerabilities cannot be patched.	Migrate affected systems to newer operating systems or removing from CPS network entirely.	Complete	An Enterprise level patching strategy has been created and shared between the Information Security group and ITM. We are targeting the next school year to being implementation of said strategy.

VoIP Security Configuration

Risk	Key Findings	Impact	Recommendation	CPS Status	CPS Response
	Telephony systems are end-of-life.	These systems are vulnerable state because new vulnerabilities will not be patched.	Develop a plan to transition to a new, supported version of the system, and to annually allocate budget to maintain the telephone system.	In Progress	Discussion have taken place between key stakeholders and a budget request has been made for upgrading the telephony systems.

Wireless LAN Penetration Testing

Risk	Key Findings	Impact	Recommendation	CPS Status	CPS Response
	Pre-shared keys are used to authenticate to the wireless network.	Pre-shared keys can be easily acquired by unapproved users and potentially used for harmful purposes.	Adopt a per-user centralized authentication method for the wireless network.	In Progress	ITM has a Network Access Controls project underway (to be completed SY21).
	Wireless infrastructure contains end-of-life hardware.	CPS may not be able to run supported software to protect from known vulnerabilities.	Eliminate end-of-life hardware and ensure that the wireless infrastructure is running supported software.	In Progress	ITM has a plan for replacement scheduled for fall/winter 20/21.
	CPS lacks security controls to enforce BYOD policy.	Personally owned devices are easily connected to the CPS network without restrictions.	Update The BYOD policy to meet the district needs and develop technical security controls to enforce the policy.	Planning Phase	Information Security will work with the appropriate stakeholders. Target dated dependent on prioritization.

Application Security

Risk	Key Findings	Impact	Recommendation	CPS Status	CPS Response
	CPS Sofware Development Lifecycle process does not include application security testing.	Application security vulnerabilities may exist and are undetected.	CPS should develop an approach to addressing security in the Software Development Lifecycle to include the following components: People, Processes, Technology.	Planning Phase	Information Security will work with the appropriate stakeholders.Target dated dependant on prioritization.
	CPS lacks a Vendor Risk Management (VRM) process for evaluating IT service providers.	CPS does not have clear visibility into potential risks associated with 3rd party suppliers.	Implement VRM process will assess, monitor and manage risk exposure from third-party suppliers that provide IT products and services to the organization.	Planning Phase	Information Security will work with the appropriate stakeholders. Target dated dependent on prioritization.

Social Engineering

Risk	Key Findings	Impact	Recommendation	CPS Status	CPS Response
	CPS lacks an effective cyber security training program.	The CPS user community does not readily recognize a phishing attempt.	Develop a comprehensive cyber security awareness training program to better equip users to recognize threats.	Complete/On Going	Recommendations from the security assessment were incorporated into additional training materials. Training was provided to Tech Coordinators and will continue to be given to targeted groups.
	CPS lacks user verification guidelines for users contacting the service desk.	Potential compromise of user accounts	Establish procedures to verify users calling the service desk before account changes are made or information is provided.	Planning Phase	Information Security will work with the appropriate stakeholders. Target dated dependent on prioritization.

A copy of the full presentation is available in the Board office.

Fiscal Year 2019 Financial Audit Report

Kevin Vaughn, Plattenburg & Associates, informed the Committee that they are engaged on behalf of the Ohio Auditor of State to audit the financial statements of the governmental activities of the Cincinnati City School District for the year ended June 30, 2019. Mr. Vaughn reviewed the results of the Single Audit Report and management letter.

A copy of the report is available via the Ohio Auditor of State website (https://www.ohioauditor.gov/auditsearch/detail.aspx?ReportID=152779), and the management letter is available in the Board office.

ACTION: Administration will provide an update at the August 26, 2020, Audit Committee meeting outlining the action plan for each item from the management letter. Paul McDole, Director of Human Resources, will provide an update regarding the retirement system as well as the independent contractor versus employee management letter items. Dan Hoying, General Counsel, will provide an update regarding the collective bargaining agreement management letter comment.

Fiscal Year 2021 Internal Audit Plan –*Internal Audit Department*

Lauren Roberts, Director of Internal Audit, presented the Fiscal Year 2021 Internal Audit Plan for approval by the Audit Committee. Ms. Roberts reviewed the following areas of the Internal Audit Plan:

Fiscal Year 2021 Risk Assessment

- Overview
- Audit Universe (a full list of areas within an organization that could be audited)
- Methodology (risk categories utilized to perform assessment)
- Risk Assessment Results (Financial, Audit, Strategic, and Entity-Level)

Fiscal Year 2021 Planned Engagements

- Advisory
  - COVID-19 School Site Audits
  - Grants Financial Management & Internal Controls
  - District Strategic Plan Support – Centralization of Processes
- Assurance
  - Continuous Auditing
- Follow Up
  - Online Learning Compliance
- Fiscal Year 2020 Internal Audit Plan – Potential Carryover Projects
  - Transportation Follow-Up
  - Payroll Follow-Up

Multi-Year Audit Cycle

- A summary of past, present and future audit engagements.

Internal Audit Development and Advancement

- Documentation of Internal Audit Procedures
- Departmental Staffing Expansion
- Professional Development

Audit Committee Chair Heldman moved to approve the Internal Audit Plan as written and Clarice Warner second the motion. The Plan was approved. A copy of the Fiscal Year 2021 Internal Audit Plan is available in the Board office.

ACTION: Audit Committee member Carol Mitchell-Lawrence requested Mr. McDole provide regular updates to the Committee regarding the progress made towards implementing the recommendations from the Benefits Internal Audit Report dated February 27, 2020.

The meeting adjourned at 6:04 pm.

Audit Committee
Thomas D. Heldman, Chair
Chatika Britton
Jennifer Couser
Jim Crosset
Christine Fisher
David Foote
Elizabeth Gutridge
Daniel E. Holthaus
Carol Mitchell-Lawrence
Clarice Warner
Eve Bolton (Finance Committee, Chair)
Melanie Bates (Finance Committee)
Ben Lindy (Finance Committee)

Staff Liaisons
Jennifer Wagner, CFO/Treasurer
Lauren Roberts, CPA, CFE, Director of Internal Audit