Collier County Public Schools, Florida
Audit Report: Top-10 High-Risk Areas of Focus

January 16, 2024

TABLE OF CONTENTS

TRANSMITTAL LETTER

January 16, 2024

The School Board of
Collier County Public Schools
5775 Osceola Trail
Naples, FL 34109

Pursuant to our approved Statement of Work executed October 10, 2023, with Collier County Public Schools ("District," "CCPS"), we hereby present the results of our risk assessment Top-10 High-Risk Areas of Focus, to assist the District in identifying and prioritizing key risks impacting its current operating environment, and the requirements of Florida Statute 1001.42.

This assessment considers 'inherent risk', which is the risk of a function in an environment void of controls. *Therefore, functions with inherently high-risk may be included in the identified Top-10 High-Risk Areas of Focus; although their inclusion does not mean 'issues' or concerns currently exist, but rather that the high-risk nature of the function is such that a higher potential exists for issues to develop.* We have provided a high-level process of each proposed audit function/area, the key potential financial, compliance, and public perception inherent risks, as well as the audit strategy for evaluating the effectiveness of the processes, procedures, and controls in place within the function.

Our Risk Profile is organized by the following sections:

Process Overview	This provides a high-level overview of our objectives, methodology, and definitions of the risk classifications applied throughout the document.
Top-10 High-Risk Areas of Focus	This section includes a listing of identified risks, including the inherent risks, risk definition, interview observations, and proposed review strategy.

In connection with the performance of these services, we have not performed any management functions, made management decisions, or otherwise performed in a capacity equivalent to that of an employee of CCPS.

We would like to thank the staff and all those involved in assisting us with this assessment to determine the District's current Top-10 High-Risk Areas of Focus.

Respectfully Submitted,

RSM US LLP

RSM US LLP

PROCESS OVERVIEW

Objectives

This process is intended to assist in analyzing risk impacting Collier County Public Schools' ("District", "CCPS") current operating environment, including inherent and residual impacts and likelihood, and to identify the key risks impacting the current operations, functions, and activities. Objectives included the following:

- Refine and update the District's risk profile previously prepared as part of the original Top-10 High-Risk Areas of Focus presented to the Board in March 2022.
- Identify and prioritize key risks impacting the District's current operating environment, functions, and activities.
- Facilitate discussions with Management regarding risk ownership and mitigation activities.
- Identify potential audit activities for the Board's consideration.

Approach

1. *Identify and Measure Risk*
   - Conducted interviews with key stakeholders to identify current risks.
   - Reviewed the District's strategic plan, financial statements, current events, and other information as deemed applicable.
2. *Prioritize Risk*
   - Evaluated the level of risk within each process area based on the frequency with which it was mentioned during the interviews and the severity of potential impact on District operations and fulfillment of objectives.
   - Evaluated risk across various classifications, such as: Reputation, Compliance, External Factors, Human Resources, Technology, Finance, Operations, and Strategic.

   Note: RSM evaluated and prioritized risks based on information gleaned from interviews, severity of impacted business operations, and interference with fulfillment of District objectives. This review did not include review of and detailed testing of source documents.
3. *Communicate Results*
   - Refined the District's current risk profile.
   - Reviewed and provided this Risk Assessment: Top-10 High-Risk Areas of Focus with Management and the Board.

Risk Classifications

Risk classifications serve as the framework for assessing and prioritizing the risk model. RSM classified each of the risks into one (1) or more of the following categories:

Compliance

Compliance with applicable laws and regulations.

External Factors

Known and emerging market trends, industry regulations, external stakeholder expectations, political, environmental, social, and technological unexpected events.

Finance

Oversight and internal controls over budgeting and forecasting, procurement, financial reporting, endowment, and utilization of resources.

Human Resources

Policies, procedures, and practices for attracting, training, and maintaining a qualified, skilled, and diverse workforce.

Operations

Effectiveness and efficiency of processes and communications across departments to achieve strategic, financial, and operational objectives.

Reputation

Ability to anticipate and mitigate risks that could adversely affect external perceptions of Collier County Public Schools.

Strategic

Executive level oversight, planning and reporting processes established to achieve strategic objectives including monitoring performance and organizational alignment to meet objectives.

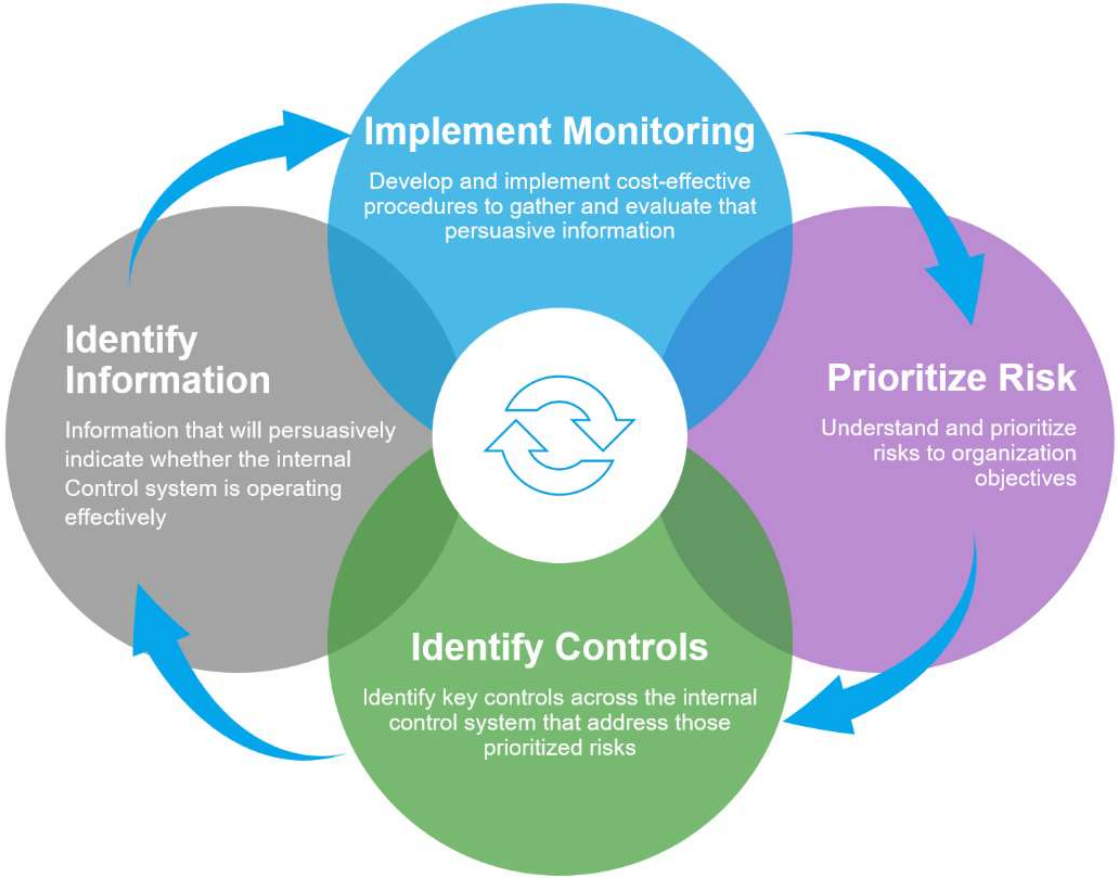
Technology

A sufficient IT infrastructure and environment to meet the needs of the District. Oversight and internal control over data integrity, business continuity, disaster recovery, data privacy, general and application controls, and cybersecurity.

PROCESS OVERVIEW (CONTINUED)

The objective of this assessment is to identify the District's current Top-10 High-Risk Areas of Focus, the purpose of which is to identify those areas determined as having a relatively high-risk profile or that otherwise require audit attention for various reasons, for the Board's consideration. This document is *on-line real-time* and labeled as *proposed* because it is a *living document*. As factors change and situations arise, the proposed top-10 can and will change. As part of this assessment, 'risk' focuses on various factors such as: financial, strategic, performance/operational, and compliance risk, as well as the general effect of public perception related to District-wide activities and initiatives.

Our approach is based on the widely accepted Committee of Sponsoring Organizations ("COSO") guidance on monitoring Internal Control Systems, as shown below:



PROCESS OVERVIEW (CONTINUED)

Our analysis of high-risk areas considers 'inherent risk', which is the risk of a function in an environment void of controls. Therefore, functions with inherently high-risk are included in this Top-10 High-Risk Areas of Focus. Their inclusion does not mean 'issues' or concerns currently exist, but rather that the high-risk nature of the function is such that a higher potential exists for issues to develop. The high-risk areas of focus listed in this profile is a point-in-time depiction and should be considered a living document. As factors change and situations inevitably arise, the risks identified can and will change.

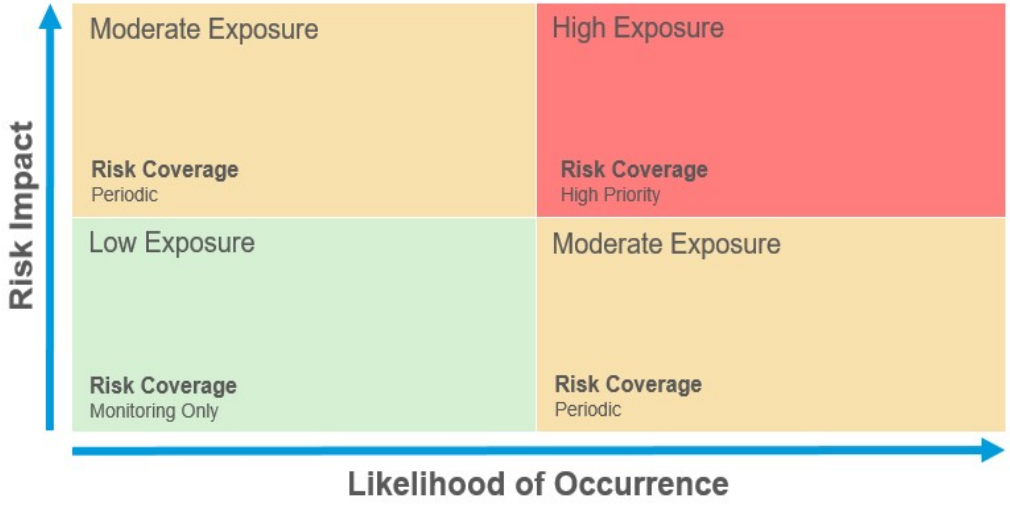
The chart below illustrates the exposure environment for positioning the District's risks and evaluating the desired response based upon the likelihood of occurrence and potential impact on operations and objective fulfillment.

Inherent Risk

- Risk of an occurrence before the effect of any existing controls.
- If you were building this process, what would you be concerned about?
- What is not preventable?

Residual Risk

- Risk remaining after the application of controls.
- Potentially reduced impact or likelihood.



PROCESS OVERVIEW (CONTINUED)

Florida Statute 1001.42, requires any School District receiving annual federal, state, and local funds in excess of $500 million to employ an internal auditor. To assist CCPSs' Board with adherence to Florida Statute 1001.42, this Top-10 High Risk Areas of Focus has been developed for the Board's consideration. In addition, and in alignment with professional standards such as the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing and AICPA consulting standards, fully functioning audit operations and function should include systematic audits selected through this process, ad hoc audits as new facts emerge, or requests by the School Board. In addition, it should include:

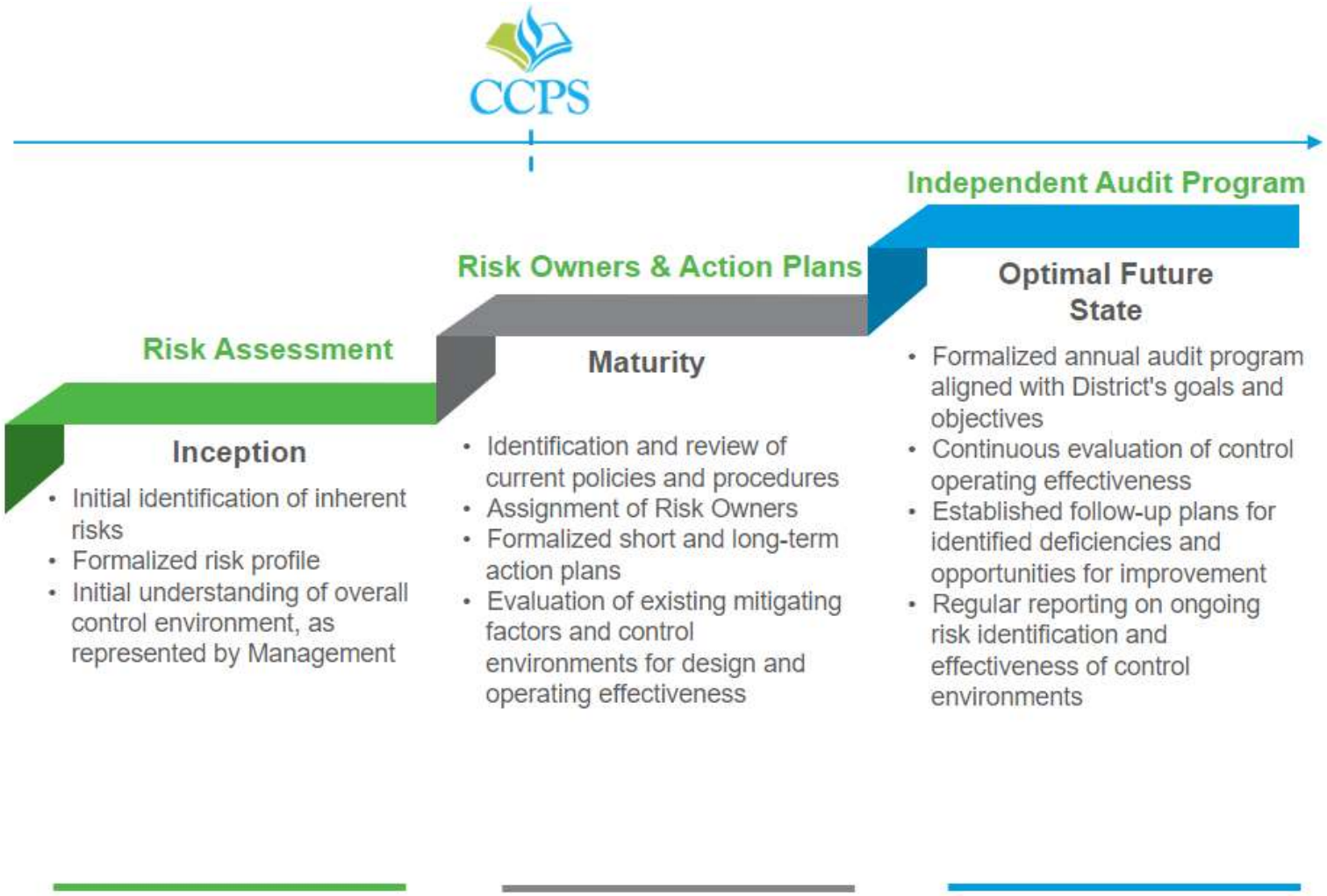
Update Risk Assessment and Audit Plan Development
Risk is not stagnant; it is constantly evolving. As factors change and situations arise, this plan can and will change. The high-risk areas of focus and proposed audit plan should be updated annually.

Follow-up Procedures
Auditors should establish a follow-up process to confirm that management actions have been effectively implemented or that Management has accepted the risk of not taking action. Included within each report provided, for each audit completed, a Management Response section will be added for Management to respond and include an action plan for remediation (if needed), as well as a targeted date of completion. Follow-up procedures will be performed after the completion date noted by Management. Follow-up typically occurs after ample time has passed with the new control/procedure in place (generally six months) to verify and report the implementation status of the recommendations and Management's action related to the previously reported findings. Periodically, we perform procedures for those issues where the target dates have been reached to verify and report the implementation status of recommendations to the previously reported findings. Follow-up reports will be presented to the Board.

Quality Control
Auditors should maintain a quality assurance and improvement program that covers all aspects of the audit activity, including appropriate supervision, periodic internal assessments, and ongoing monitoring of quality assurance. RSM's quality control processes specific to public sector clients include, when applicable, concurring partner review (independent of the engagement) and, when necessary, consultation with the District General Counsel prior to reports being issued into the public record.

PROCESS OVERVIEW (CONTINUED)

The results of this assessment will be presented to the Board and will provide the District with an overview of the current risk environment. Next steps typically include utilization of this profile to enhance awareness of existing risks and to formulate the next audit plan.



RESULTS

The following is a summary of identified risks. The first four are listed as most significant based on the frequency of mention during our interviews, and professional judgement. The remaining risks are listed in alphabetical order and should be considered comparable in severity. *We would like to re-iterate, as previously noted in this document, that the inclusion of a proposed high-risk area of focus does not mean 'issues' or concerns currently exist, but rather that the high-risk nature of the function is such that a higher potential exists for issues to develop.*

Top-10 High-Risk Areas of Focus
❖ Purchasing and Procurement Compliance
❖ Recruiting and Onboarding
❖ Information Technology – Data Protection
❖ Cybersecurity – External Penetration Testing
❖ Budgeting
❖ Information Technology General Controls
❖ Maintenance
❖ Physical Security
❖ Purchasing Cards
❖ Student Discipline

RESULTS (CONTINUED)

Risk Classification	Purchasing and Procurement Compliance
Compliance External Factors Finance Operations Reputation Strategic Technology	**Risk Definition:** The purchasing function serves as a resource for the School District to acquire necessary goods and services, achieve economies of scale, facilitate strong business relationships with vendors, negotiate competitive pricing, and protect public funds. The Purchasing Department is a central hub of purchasing power for all other departments and schools, and must work closely with the District's General Counsel to confirm purchasing agreements adequately protect the District from risk. The Department is also responsible for facilitating competitive procurement methods, confirming vendors are consistently and uniformly evaluated, and reviewing purchases of various thresholds so that the appropriate approval is obtained, as required by law. **Inherent Risks:** Outdated, inadequate or undocumented policies and procedures; ineffective scope development; non-compliance/improprieties with Florida Statutes and District policies for solicitation and procurement; purchases not properly authorized; purchases not made for legitimate business needs; inadequate segregation of duties; legal ramifications; and bid protests. **Review Strategy:** To evaluate the design and control structure, including adherence to policies and procedures, for operating effectiveness. This may include areas such as assessing compliance with authorization, solicitation, selection, and contract execution with vendors/suppliers per Florida Statute and District policies and procedures; evaluating sufficiency and adequacy of the documentation and records to support the procurement; and appropriateness of access controls and segregation of duties within the purchasing function.

RESULTS (CONTINUED)

Risk Classification	Recruiting and Onboarding
Compliance External Factors Finance Human Resources Operations Reputation Strategic Technology	**Risk Definition:** One of the most critical activities of a high-functioning Human Resources Department is the ability to recruit qualified candidates, execute successful, efficient, and complete onboarding processes, and adhere to approved compensation procedures. Employee recruiting and onboarding refers to the procedures taken when employee candidates are sought, identified, evaluated, interviewed, selected, and integrated into District operations. This process also includes working collaboratively with different departments to obtain relevant employee data, including state-required information, and provide required training and orientations through the employee's first day of employment. Compensation setting procedures include actions taken to calculate, support, approve, and communicate an individual's base pay to employees and hiring managers. During fiscal year ending June 30, 2023 ("FY23") the District processed approximately 1,770 new hires. These factors make the Human Resources department an inherently high-risk function, from a financial, operational, compliance, and public perception perspective. **Inherent Risks:** Outdated, inadequate or undocumented policies and procedures surrounding job posting, recruiting, screening, and offers of employment; interdepartmental collaboration is ineffective; onboarding processes are inefficient; candidate vetting procedures are inadequate or inappropriate; new hire approval process in inconsistent or incomplete; compensation decisions do not receive proper approval; employees are hired who are not adequately screened and/or qualified; and non-compliance with applicable policies, laws and regulations. **Review Strategy:** To assess the following areas: recruiting, selecting, onboarding of employees, and approval of compensation. Aspects of the assessment would include testing over the following areas: timeliness of job postings, documentation of employee screening and interviews, use of review checklists and/or matrixes, completion of required pre-employment consent forms, the performance of necessary background check activities, candidate vetting, the orientation process, and an assessment of the overall timeliness to fill positions.

RESULTS (CONTINUED)

Risk Classification	Information Technology – Data Protection
Compliance	**Risk Definition:**
External Factors	An assessment of data protection includes a deep dive into the nature of and protective measures used for sensitive data (ex: student data, personally identifiable information, etc.) Privacy concerns exist wherever sensitive information is collected, stored, used, and finally destroyed or deleted – in digital form or otherwise. As laws and regulations surrounding data protection are constantly changing, it is critical to keep abreast of any changes in laws/regulations and continually reassess compliance with data privacy and security regulations. The District's business platforms and student information system are critical for employees, administrators, teachers and students to perform a variety of day-to-day functions and responsibilities. These systems store a variety of sensitive data including names, dates of birth, social security numbers, home addresses, grades and course history, and health data.
Finance	Data protection includes, but is not limited to, the encryption of data within the systems, the encryption of data when transmitted outside of the systems, restriction of sensitive data movement via email or removable media, restriction and monitoring of privileged/administrator user access, and implementation of network firewalls and intrusion detection/prevention solutions and the appropriate segregation of duties for users with the ability to develop and migrate production-level changes to source code.
Human Resources	**Inherent Risks:**
Operations	Failure to complete strategic IT goals and initiatives; inability to meet organizational goals; non-compliance with regulatory standards; unauthorized access to sensitive data; data is compromised or lost; access to information is untimely for critical decision-making activities; inability to identify anomalies or issues in data quality; review of infrastructure, platforms, and applications that house sensitive data is improper or insufficient; duties are not properly segregated; and financial loss, reputational damage, and operational disruption or failure.
Reputation	**Review Strategy:**
Strategic	To assess and identify areas of risk associated with protection of sensitive data that could cause harm to the District. This review would focus on sensitive data protection standards, controls, and technologies designed to protect sensitive information. Specific focus areas may include review of logical access, privileged access, user access review processes, segregation of duties, change management, review of applicable policies and procedures, network security, and physical security of servers and/or databases.
Technology	

RESULTS (CONTINUED)

Risk Classification	Cybersecurity – External Penetration Testing
Compliance External Factors Finance Operations Reputation Strategic Technology	**Risk Definition:** Cybersecurity is an important priority within the public sector. Threats are constantly changing and evolving; thus, this area is inherently high-risk. Organizations like the District are under constant attack from external threats. As attack methods have evolved, so have the requirements for safeguarding user, student, and District information. Likewise, it is important to measure the security of technology assets to understand the ability to defend against threats. Performing a penetration test can help identify an organization's security posture and configuration standards through assessing the resiliency of the external network against a determined attacker. Typically, a penetration test should be performed at least annually to stay abreast of new and evolving attacks. Developing and maintaining an effective Information Security program is critical for the District's ability to achieve its objectives. Furthermore, the risk of data breach or misuse of sensitive data could result in significant damage to the District's reputation, financial standing, and operational capability. RSM is scheduled to perform an internal penetration test January 2024. **Inherent Risks:** Undetected threats and attacks to District systems; loss or manipulation of critical data; systems and applications are not configured appropriately to support proper maintenance and monitoring (closed-loop feedback); District data is not being stored securely; outdated, inappropriate, or incomplete response plans to ransomware/malware attacks, business email compromises (i.e. phishing or social engineering emails), and/or data thefts; monetary losses resulting from the cyberattack or litigation subsequent to the cyberattack; and time and resources may be inefficiently spent manually analyzing threats to District systems. **Review Strategy:** To assess current security controls in an effort to determine the actionable impact from an attacker attempting to bypass perimeter security controls and accessing the internal network or sensitive data. The focus of penetration testing is not to prove that the network is free of all vulnerabilities; rather, the focus is to validate the organization's security posture and configuration standards through assessing the resiliency of the internal network against a determined attacker. This level of testing relies heavily on techniques and toolsets favored by real-world threat actors in order to closely simulate an attack scenario, and leverages both manual and automated testing methods.

RESULTS (CONTINUED)

Risk Classification	Budgeting
Compliance External Factors Finance Human Resources Operations Reputation Strategic Technology	**Risk Definition:** The District's Budget Department plans, manages, and oversees the District's annual budget preparation and monitors compliance with state budget adoption and reporting requirements. As part of the annual budget process, each of the District departments meet with Budget staff and the Deputy Superintendent to review requests related to existing projects, new projects, travel, supplies, etc. Once the District's annual budget is adopted, the Budget Department continuously monitors transactions to confirm that the budget is efficiently allocated and properly recorded. Budgetary controls are established utilizing a position control system for school personnel based on projected enrollment and at the District, level using historical trends and forecasting models, and budgets across the District are reviewed each year through collaboration with all departments and review from the Board. **Inherent Risks:** Budget calculations contain unintentional errors; data entry procedures, including secondary reviews, are incomplete or inadequate; budgets are intentionally manipulated or misreported; budget rationale, status, and amendments are not communicated appropriately or timely; increased exposure to operational disruption; contractual and legal risk; reputational damage; and non-compliance with governing authorities. **Review Strategy:** To evaluate traditional budgeting processes, which includes an assessment of the adequacy and effectiveness of internal controls over budget development, monitoring, reporting, and modifications. Procedures would include a review of budget modification and amendment processes for appropriateness and proper authorization; verify proper segregation of duties between budget preparation, approval, execution, and accounting/reporting; evaluate how data is obtained, reviewed, verified for accuracy, and reported; and evaluate the timeliness, accuracy, and usefulness of budget status reports and communications.

RESULTS (CONTINUED)

Risk Classification	Information Technology General Controls
Compliance External Factors Finance Operations Reputation Technology	**Risk Definition:** Information Technology General Controls (ITGC) are the basic controls that can be applied to IT systems such as applications, operating systems, databases, and supporting IT infrastructure. The objectives of ITGCs are to review and protect the integrity of the data and processes that the systems support. The most common ITGCs include: Logical Security and Security Administration, Change Management, Program Development, and Computer Operations. Because ITGCs are considered the foundation of an automated control environment, which ultimately supports key organizational objectives, they are inherently high-risk. As technology advances and changes within the District through the introduction of new people, processes, applications, and systems, the underlying ITGCs must be evaluated to confirm they are still designed and operating effectively. **Inherent Risks:** Unauthorized or inappropriate access to District system resources and data; inappropriate or unintended changes to critical systems and applications; inadequate backups and availability of critical data and systems; and data theft. **Review Strategy:** To assess the control design and operating effectiveness of the IT general controls domains for the in-scope applications. The assessment of IT risk and controls addresses the key requirements of the Federal Financial Institutions Examination Council (FFIEC) and follows the guidelines of Control Objectives for Information and related Technology (COBIT), the baseline requirements of Cybersecurity Assessment Tool (CAT), and other examination standards, such as the Gramm-Leach-Bliley Act (GLBA), FDIC Information Technology Risk Examination (InTREx), and FDIC FIL-81-2005 Procedures for Assessing Information Technology Risk.

RESULTS (CONTINUED)

Risk Classification	Maintenance
Compliance External Factors Finance Operations Reputation Strategic Technology	**Risk Definition:** Work order management is a crucial component of efficiently keeping school sites safe, preventing costly damage through scheduled preventative maintenance, and maintaining compliance with SREF (State Requirements for Educational Facilities) and the Florida Building Code. The maintenance work order system is located in Facilities Management under District Operations. The maintenance work order system includes, but is not limited to submitting a work order, tracking work order fulfillment and prioritization, inventory storage, pay applications, and the allocation of maintenance expenditures, including employee time spent and inventory/parts used. The District currently utilizes a wholly customized work order management system called Atlas to manage, monitor, and facilitate work orders within the Facilities Management team. While fully customized programs are tailored to the District's specific needs, the unique nature of the technical environment may cause difficulty in finding replacement software or in implementing compatible ancillary modules. Additionally, the individual programmer was originally contracted with the District over ten (10) years ago, and as such a retirement, software sale, or unforeseen disaster, may limit the District's ability to receive systematic updates, upgrades, or solutions to functionality issues. Work order management is a crucial component of efficiently keeping school sites safe, preventing costly damage through scheduled preventative maintenance, and maintaining compliance with SREF (State Requirements for Educational Facilities) and the Florida Building Code. **Inherent Risks:** Outdated, inadequate or undocumented policies and procedures; non-compliance/improprieties with Florida Statutes and District policies for solicitation and procurement; unreported conflicts of interest; non-compliance with vendor contract terms; failure to meet select contract provisions; vendor favoritism; non-performance of vendors; inaccurate accumulation or allocation of time and materials to work orders; ineffective monitoring and reconciliation of the work order system; inadequate monitoring of work order distribution, production and / or overtime; untimely response to and priority of work orders and needs of the District; and inadequate monitoring of key performance indicators, such as work order turnaround, employee productivity, and parts utilization. **Review Strategy:** To assess maintenance standard operating procedures to determine whether they are sufficient and cover the numerous aspects of the maintenance work order system, including the work order process and associated controls. The review will also include detailed testing of sampled work orders and their relevant approvals, expenditures, and prioritization, and adherence to preventative maintenance work order schedules.

RESULTS (CONTINUED)

Risk Classification	Physical Security
Compliance External Factors Finance Human Resources Operations Reputation Strategic Technology	**Risk Definition:** School districts have been facing a heightened degree of physical threat, whether from crime, natural disaster, technology incidents, or human error. Physical security is the protection of people, property, and physical assets from actions and events that could cause damage or loss. Just as cybersecurity is critical for protecting systems and data, physical security is equally important for protecting people and assets. A physical security assessment is a foundational and effective review of an organization's security program. **Inherent Risks:** Physical harm to students, employees, and visitors; property and assets are exposed to theft and destruction; unauthorized access to information systems; non-compliance with Florida Statutes; outdated, inadequate or undocumented policies and procedures; exposure to legal ramifications; inability to sufficiently monitor school operations; operational inefficiencies or failure; and reputational damage. **Review Strategy:** To evaluate whether certain physical controls are in place, effective, and functioning as intended specific to the Administration Building. The review will include cycling through unscheduled walk-throughs of selected District sites, probe perimeter defenses, and entrance access to uncover any major gaps and vulnerabilities. Coordination with the appropriate District personnel is imperative to safely and effectively evaluate the physical controls in place. We will further refine the review strategy with the Safety and Security Department and with District leadership.

RESULTS (CONTINUED)

Risk Classification	Purchasing Cards
Compliance External Factors Finance Operations Reputation Technology	**Risk Definition:** Purchasing Cards ("P-Cards") exist to give organizational leaders autonomy and efficiency in purchasing goods and services necessary to the continuation of business operations. These tools shield department and school leadership from lengthy approval processes when time is of the essence and allow purchases to be made with unencumbered funds or purchase orders. Because purchases are reviewed and approved after the expenditures have been made, p-card use is inherently high-risk. Robust policies, procedures, and review processes are essential to detecting and preventing inappropriate purchases. During fiscal year ending June 30, 2023 ("FY23"), the District spent $6,427,090[1] through use of the 210 active P-Cards. **Inherent Risks:** Outdated, inadequate or undocumented policies and procedures surrounding employee usage, supervisor review/approval, vendor payments, inventory of P-Cards, etc.; P-Cards are not securely stored and monitored; duplicate payments of vendor invoices are not monitored; controls or segregation of duties for approving, furnishing and reconciling P-Cards are not adequate; reconciliation of invoices is not being performed timely; and fraudulent spending and use of P-Cards. **Review Strategy:** To assess management's design and effectiveness of internal controls over the use of purchasing cards. This would include an examination of compliance with existing policies and procedures, and applicable regulatory requirements, and identification of process gaps, if any, and opportunities for improvement. The approach may include integration of data analytics by card or user, as well as the vendor spend to identify irregularities, prohibited transactions, duplicative transactions, or split transactions.

[1] This information is unaudited.

RESULTS (CONTINUED)

Risk Classification	Student Discipline
Compliance External Factors Finance Human Resources Operations Reputation Strategic Technology	**Risk Definition:** School districts across the country are reporting an increase in student behavior incidents that is resulting in discussions to help identify contributing factors and solutions. External factors identified include the COVID-19 pandemic and its impact on education, mental health, class size, staff turnover and vacancies, and evolving discipline strategies by both parents and educational agencies. **Inherent Risks:** Outdated, inadequate or undocumented policies and procedures; disciplinary procedures are done inconsistently; non-compliance with District policies and State regulation; behavioral incidents are undocumented or incompletely documented; inability to accurately report disciplinary events; lack of monitoring processes; data regarding student incidents in incomplete or lacks integrity; and manual and inefficient disciplinary processing procedures resulting in operational downtime. **Review Strategy:** To assess compliance with certain board policies related to student discipline, perform data analytics with available data, and survey key CCPS stakeholders to provide relevant information regarding the culture encompassing student discipline to the Board to allow for future decision making. Testing procedures may include, but may not be limited to, selecting a sample of referrals from available datasets to evaluate the accuracy of referral data, evaluate the timeliness between the actual incident date and the incident documentation, evaluate the completeness of the discipline referral form, review documentation to assess whether correction action administered was successfully completed and that documentation existed to support all actions, evaluate the level of severity of the corrective actions administered was compliant with CCPS discipline policies, and verify incidents were communicated and reviewed when applicable.

RSM US LLP
7351 Office Park Place
Melbourne, Florida 32940
321.751.6200
www.rsmus.com