School District of
OSCEOLA COUNTY
FLORIDA

School District of Osceola County, Florida

Risk Assessment to Develop Proposed Fiscal Year 2022-23 Internal Audit Plan

July 26, 2022

RSM

TABLE OF CONTENTS

Transmittal Letter 1

Risk Assessment 2

Proposed Top 10 High Risk Areas for Internal Audit 4

School District of OSCEOLA COUNTY FLORIDA

TRANSMITTAL LETTER

RSM

July 26, 2021

7351 Office Park Place
Melbourne, Florida 32940
T 321 751 6200
F 321 751 1385
www.rsmus.com

Audit Advisory Committee
School District of Osceola County, FL
817 Bill Beck Blvd.
Kissimmee, FL 34744

Pursuant to our Statement of Work dated June 21, 2022, we hereby submit the risk assessment for the development of the proposed internal audit plan for the School District of Osceola County, Florida ("District") for fiscal year 2022-23 ("FY23").

We performed the risk assessment by applying a broad-based, business view of risk, linked to the annual budget, financial reports, and operations. We reviewed recent board meeting minutes and various media sources to understand the District's current environment. We conducted interviews with District School Board Members, Superintendent, and other members of management to gain an understanding of "What keeps them up at night?" and narrow in on their objectives and identified risks. For the purpose of this risk assessment, 'risk' focuses on financial, strategic, performance/operational, and compliance risk, as well as the general effect of public perception with regard to District-wide activities and initiatives. During the interviews, we discussed and identified areas of high risk, opportunities, and vulnerabilities. As a result, we are presenting the Proposed Top 10 High Risk Areas for Internal Audit ("Proposed Top 10"). These are on-line real-time and are labeled as proposed because it is a living document. As factors change and situations arise, the Proposed Top 10 can and will change.

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 the District. We would like to thank the District's School Board, Superintendent, members of leadership, as well as the various departments and staff involved in assisting with the risk assessment process.

Respectfully Submitted,

RSM US LLP

INTERNAL AUDITORS

RISK ASSESSMENT

The objective of this assessment is to identify and develop a proposed internal audit plan: 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. 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 the proposed internal audit plan. 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 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 priority of risk concerns. A proposed internal audit plan generally focuses on areas or functions that are high exposure and high priority (the upper right quadrant).

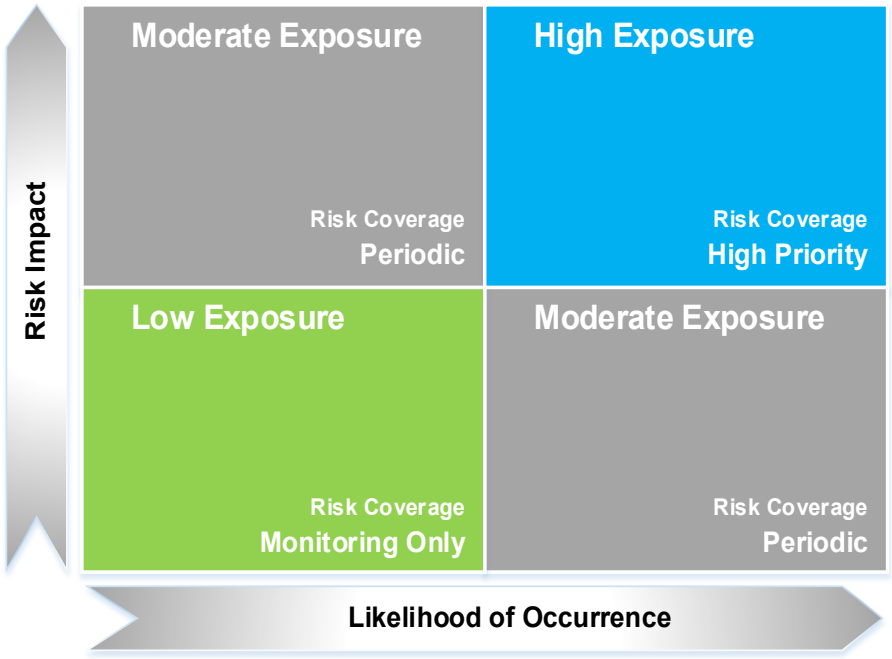
Inherent Risk

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

Residual Risk

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

Our risk assessment was conducted utilizing a broad-based business view of risk. We conducted interviews with District School Board members to gain an understanding of their perspective of risk at the District, focusing on their objectives in order to identify potential risks. We also conducted interviews with the Superintendent and other members of upper management to identify risks, vulnerabilities, and potential opportunities. We reviewed recent media coverage, as well as recent School Board meeting agendas, minutes, and other available documentation.



RISK ASSESSMENT - CONTINUED

Our approach primarily defines 'Risk' in a government entity as Financial and Compliance-related risk, as well as Public Perception risk. Strategic, Performance and Operational risks are also considered. We evaluated the level of risk present in each area / function, across a standard spectrum of industry-accepted risk categories as follows:

CONTROL ENVIRONMENT	Describes the overall tone and control consciousness of the process / function. It involves the integrity, ethical values, and competence of personnel as well as management philosophy and operating style.
CHANGE	Addresses the extent to which change has impacted or is expected (in the near term) to impact the process / function, including changes in key personnel, statutes, the organization, its products, services, systems, or processes.
PROCESS RISK	Addresses the inherent risk of the activities performed by the process / function, including the assets managed or in the custody of the process / function. Process risk addresses the extent of support the process / function provides to vital the District functions, including the threat to continuity of the District caused by failures or errors: the probability of failure due to the amount of judgment, academic, or technical skill required to manage the unit or perform key activities.
EXTERNAL FACTORS	Describes the environment in which the process / function operates and the type and amount of external interaction in which the process / function engages. Factors to consider include overall the District and regulatory environment, the level of interaction with stakeholders and success in satisfying their requirements, the financial reporting environment, and results of regulatory compliance audits.
REVENUE SOURCE / MATERIALITY	Describes resources available and expended by the process / function. Factors to consider include the originating source of funds for a process / function, function budget, function spend, availability and use of other resources, and significance of impact to the overall operation of the District.

The internal audit function should include a balance of all types of internal audits and reviews. As such, an internal audit plan should include: Overall Audit Functions, Cycle Audits, District-wide Audits, Individual Function Audits, and may include Special Requests. We have included the Proposed Top 10 from which the School Board can prioritize a potential internal audit plan for fiscal year 2023. This includes an overview for each process as well as a summary of the internal audit strategy for each audit, subject to modification during the initial planning stages and scoping of each audit and subsequent discussions with management.

RESULTS

The following is a summary of identified risks. *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.*

Proposed Internal Audit Plan: Top 10 High-Risk Areas of Focus
1. Cybersecurity & Privacy – Penetration Testing
2. Cybersecurity & Privacy – Incident Response Playbook
3. Cybersecurity & Privacy – Social Engineering
4. Operations – Maintenance Services and Work Order Processes
5. Business & Fiscal Services – Stimulus Funding
6. Business & Fiscal Services – Property Control
7. Business & Fiscal Services – Payroll
8. Operations – White Fleet Operations
9. Districtwide – Contract Compliance
10. Business & Fiscal Services – Purchase Cards ("P-Cards")

In addition to the auditable areas above, we will also perform annual follow-up testing. We will perform follow up testing procedures on open, identified observations from previously issued audit reports. The objective of follow-up testing will be to determine whether established management action plans to remediate identified risks and observations have been successfully implemented, and effectively mitigate the risks identified.

PROPOSED TOP 10 HIGH RISK AREAS FOR INTERNAL AUDIT

The objective of the risk assessment is primarily for the development of a proposed internal audit plan for FY23. The Proposed Top 10 will assist the District in creating an internal audit plan with sufficient and continuous internal audit coverage of those areas judged as having a relatively high-risk profile or that otherwise require internal audit attention for various reasons.

1. Cybersecurity & Privacy – Penetration Testing

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 attackers. The prospect of finding that an attacker has penetrated the District's defenses and is able to steal data from the District's network keeps most leaders up at night. As threats to data and systems 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. We last performed penetration testing in June 2022 and we recommend the District perform this testing annually.

Internal Audit Strategy

The objective of *internal* penetration testing is to assess current security controls in an effort to determine the actionable impact from an attacker gaining access to the internal network. The objective of *external* penetration testing is 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.

PROPOSED TOP 10 HIGH RISK AREAS FOR INTERNAL AUDIT – CONTINUED

2. Cybersecurity & Privacy – Incident Response Playbook

Organizations like the District are under constant attack from external attackers. The prospect of finding that an attacker has penetrated the organization's defenses and is able to steal data from the organization's network keeps most leaders up at night. As threats to data and systems have evolved, so have the requirements for safeguarding user, student, employee, and District information. The processes and people that support the security of technology are the key components in protecting these valuable business assets. Likewise, it is important to measure the security of technology assets to understand the ability to defend against threats.

To keep up with a myriad of cybersecurity threats, organizations need to have a formal plan to assist in responding to a cyber-incident. Regardless of the level of planning and preparation, no organization is completely safe against cyberattacks. Hence, organizations need an incident response playbook ("IRP") that identifies possible cyberattacks and the District's step-by-step plan how to respond. Performance of tabletop exercises during this process will enable the District to verify their IRP is well rounded. The District's IS Department is currently exploring the development of an IRP. Given the increasing complexity and number of cybersecurity incidents occurring within school districts across the country, the risks of harm to the District's reputation and finances is increasing.

Inherent risks may include: 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.

Internal Audit Strategy

This internal audit would include a review of the District's current IRP and evaluate the effectiveness and maturity of their Incident Response ("IR") program. This includes reviewing documents referenced in the IRP surrounding notification and escalation procedure, impact and prioritization methods, disaster recovery and business continuity plan documentation, backup restoration procedures, detection and response mechanisms, and tactical incident handling instructions.

PROPOSED TOP 10 HIGH RISK AREAS FOR INTERNAL AUDIT – CONTINUED

3. Cybersecurity & Privacy – Social Engineering

Social engineering is a technique that relies on weaknesses in human nature, rather than weaknesses in hardware, software, or network design. Attacks are successful because they target basic human nature. While systematic controls may exist, there is still a reliance on human controls. Humans are susceptible to persuasion and manipulation through various methods.

Organizations are becoming increasingly aware that traditional technical security approaches, such as vulnerability and penetration testing, are not sufficient alone. Attackers are moving away from the purely technological attack and including an organization's personnel as a way to penetrate that organization. Social engineering tests a company's security awareness and employee compliance with the existing security policy. The purpose is to gain a better understanding of the nontechnical security posture of an organization. Social engineering enables companies to evaluate their environment's defenses when faced with complex threats that are the source of data breaches. Social engineering typically applies to using deception and testing methods to gain access to data, systems, and applications. Techniques used with this approach press people into unknowingly performing actions or divulging confidential information on behalf of an attacker.

Internal Audit Strategy

A social engineering review could occur in person or remotely, and via technical and nontechnical approaches. A variety of social engineering techniques could be employed to gain information that can be used to compromise an organization. Examples of the social engineering services that could be deployed include:

- Email – We send a variety of email messages to select personnel to see if they will reply to messages of a questionable nature. These can include malicious attachments, spam filter checks, pharming and phishing.
- Walk-in impersonation – A RSM security consultant impersonates one of a variety of business services personnel, such as a telecommunication technician or copier repair person, to gain access to your facility.
- Call-in impersonation – Performed over the telephone, this test is best used for larger organizations where personnel do not know all employees. As with the email tests, the caller attempts to obtain information over the phone or have it sent via email or other means. Pretexting phone calls or SMS phishing or pharming techniques can also be used.
- Malicious website – This test involves email and a website. Targeted personnel are sent an electronic message instructing them to visit the malicious or harvesting website (for example, your organization is conducting a survey). Employees are asked to log on to the website using their internal network credentials. The website then counts the number of people who connect and counts who logs in. We can also perform a social networking site inspection.

PROPOSED TOP 10 HIGH RISK AREAS FOR INTERNAL AUDIT - CONTINUED

4. Operations – Maintenance Services and Work Order Processes

The District's Maintenance Department is responsible for sustaining a safe, sanitary, and functional environment for the students and employees of the District. The function oversees the repair and upkeep of District grounds, buildings, and equipment. Timely repair and preventative maintenance of these assets will prolong their useful life and potentially reduce the future cost of renovation, repair and / or replacement. Although many preventative and repair functions are performed with in-house labor, the size and scope of maintenance throughout the District requires the use of third-party vendors for certain services. Work orders are used to manage, organize, and track the work performed. A critical piece of the maintenance process is control around accumulating and properly allocating the maintenance expenditures, such as employee time spent, and inventory / parts used for specific projects.

Inherent risks include: 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.

Internal Audit Strategy:

This audit will be designed to assess whether the system of internal controls is adequate and appropriate within the Maintenance Department for promoting and encouraging the achievement of management's objectives in the categories of compliance with applicable laws, administrative rules, and other guidelines. The review may focus on the Maintenance Department's process for procurement of goods and services; management and administration of vendors and contracts; monitoring processes; work identification and prioritization; work completion and review; utilization of work order system; and internal performance monitoring.

PROPOSED TOP 10 HIGH RISK AREAS FOR INTERNAL AUDIT - CONTINUED

5. Business & Fiscal Services – Stimulus Funding

To address the impact COVID-19 on schools, federal funding was provided to direct support to state education agencies (SEA) and local education agencies (LEA). This funding was directed and subsequently expanded through the following acts of congress:

1. The Elementary and Secondary School Emergency Relief (ESSER) Fund was established as part of the Coronavirus Aid, Relief, and Economic Security (CARES) Act in March 2020, and provided $13.5 billion in ESSER funding to SEAs and LEAs to address the impact of COVID-19 on elementary and secondary schools.
2. In December 2020, ESSER funding was expanded through the enactment of the Coronavirus Response and Relief Supplemental Appropriations (CRRSA) Act. This funding provided an additional $54.3 billion for the ESSER Fund and were provided to safely reopen and sustain the safe operation of schools and continue to address the impact of the COVID-19 pandemic on the nation's students.
3. In March 2021, a third round of funding was added to the ESSER Fund through the enactment of the American Rescue Plan (ARP) Act. The ARP ESSER package included $122 billion for the ARP ESSER Fund. Funding was provided to direct aid to LEAs to help safely reopen schools and accelerate learning and mitigate learning loss. ARP ESSER allows LEAs broad discretion in determining those needs and encourages building long-term systems of support to modernize and sustain school improvements and address the impact of COVID-19.

The District is responsible for maintaining an efficient and effective system for monitoring the stimulus funding received and expended. General guidance is provided by the Department of Treasury outlining the permitted uses of stimulus funds, as well as documentation requirements in place for substantiating expenditures approved using stimulus funding. The design and operating effectiveness of key internal controls (i.e., review and approval procedures, determination of expenditure appropriateness, accounting procedures, etc.) is imperative to remaining in compliance with the evolving regulatory requirements, especially as the District is projected to receive a significant increase in grant funding as a result of the COVID-19 pandemic.

Inherent risks include: Non-compliance with state and federal regulations; misuse of funding resulting from inappropriate expenditures; inability to accurately forecast non-recurring and recurring costs associated with stimulus funds; inability to accurately and timely report expenditures; lack of appropriate evidence to support the eligibility and approval of expenditures; insufficient document retention procedures; reputational damage resulting from ineffective oversight of funding.

Internal Audit Strategy:

The primary objective of this review would be to evaluate the system in place for managing stimulus funding including key internal controls such as review and approval procedures, documentation requirements, accounting procedures, and other relevant procedures in place for maintaining compliance with regulatory guidelines.

PROPOSED TOP 10 HIGH RISK AREAS FOR INTERNAL AUDIT - CONTINUED

6. Business & Fiscal Services – Property Control

Effective property control practices are critical to ensure accurate records are maintained to capture and track all relevant asset information. The mission of the Property Records Department is to establish and promote measures that will enable the District to adequately safeguard and account for all of its property and comply with all applicable state, federal, and School Board rules, regulations, and procedures. This involves coordinating the annual physical inventory, recording acquisitions, deletions, and other changes into the Terms Asset Management database files in a timely and appropriate manner; managing the transfer and disposition of surplus property; and providing the appropriate property related information and training to School District departments and schools.

Inherent risks include: Outdated, inadequate, or undocumented policies and procedures; Inadequate controls to detect fraud, waste, and abuse; Inadequate segregation of duties; Non-compliance and inconsistencies with policies and procedures; and Ineffective accounting and administrative controls over tracking, recording, monitoring, and reporting of District property.

Internal Audit Strategy:

The primary objectives of the audit will be to analyze the current asset records, with a focus on design and effectiveness of the processes and internal controls designed to add and remove assets from the property record, accurately record the value of assets, physically safeguard assets, perform inventories of assets on a periodic basis, and the retirement and disposition of assets.

7. Business & Fiscal Services – Payroll

A primary objective of the Payroll Department is to provide for the accurate and timely payment to employees while complying with state and/or federal laws. The District employs over 7,300 employees across its various schools and departments. A significant portion of the District's budget is comprised of payroll costs and the related taxes and benefits. These salaries and benefits comprise approximately 64.2% of the total estimated operating budget.

Inherent risks include: Outdated, inadequate, or undocumented policies and procedures; Inadequate controls to detect fraud, waste, and abuse; Inadequate segregation of duties; Non-compliance and inconsistencies with policies and procedures; Employees paid for time not worked or approved; Potential for human error; Inadequate documentation and retention of timekeeping records; and Ineffective accounting and administrative controls over tracking, recording, monitoring, and reporting.

Internal Audit Strategy:

The primary objective of this audit would be to evaluate and assess whether the internal control structure of time recording, monitoring, and reporting is appropriately designed and operating effectively to pay employees timely and accurately. An audit of Payroll processes would cover the procedures performed after the time is entered and submitted by the Departments through payout to the employees.

PROPOSED TOP 10 HIGH RISK AREAS FOR INTERNAL AUDIT - CONTINUED

8. Operations – White Fleet Operations

The District manages many types of vehicles which include busses, vans, trucks, cars, and equipment. The fleet of vehicles utilized by District employees, for the purpose of District responsibilities, are referred to as the "white fleet." The Transportation Department is responsible for managing and monitoring the District white fleet.

Inherent risks include: Operational disruption or failure; financial loss; reputational damage; inability to meet strategic District growth goals; inadequate segregation of duties, inadequate safeguarding of vehicles, non-compliance with policies and procedures.

Internal Audit Strategy

The primary objective of this audit would be to evaluate fleet management processes and internal control structure to assess the efficiency and effectiveness of fleet management processes including, but not limited to; vehicle purchases, vehicle assignment, vehicle retirement, and maintenance procedures.

9. Districtwide – Contract Compliance

Contract compliance encompasses all contractual agreements, including but not limited to vendor agreements. It includes those activities performed from the time a contract is executed until the work has been completed and accepted, payment has been made, and disputes have been resolved. Although certain aspects of the purchasing function are centralized within Purchasing, many of the high-risk areas like contract administration and monitoring are decentralized to the individual departments/contract owners.

Inherent risks include: Inappropriate spending due to non-compliance with contract terms, potential conflicts of interest, and failing to meet select contract provisions. These factors and the materiality of vendor contracts make this process high risk from a financial, compliance and public perception perspective.

Internal Audit Strategy

This audit would be designed to assess whether the system of internal controls is adequate and appropriate for effective contract compliance, with selected provisions of the contract as it relates to payment for goods/services, and assess the District's monitoring processes for opportunities for improvement. We will select a sample of high-risk contracts to test in detail for compliance with the effective agreement terms and conditions, including pricing and invoicing to the District, as well as adherence to any right to audit clauses and required insurance coverage, and other potential risks to the District as appropriate.

PROPOSED TOP 10 HIGH RISK AREAS FOR INTERNAL AUDIT - CONTINUED

10. Business & Fiscal Services – Purchase Cards ("P-Cards")

A P-Card is a form of a charge card that allows goods and services to be procured without using a traditional purchasing process. They are typically issued to employees who make low dollar, high volume transactions. By using a P-Card, the District's purchasing teams can focus their efforts on more strategic high value transactions. A P-Card program is designed to enable the District to make purchases quickly and efficiently, thereby reducing the volume of invoices and request for checks being processes. There can be significant risks with P-Cards if the policies and procedures are not established correctly and are not functioning as designed.

Inherent risks include: Outdated, inadequate, or undocumented policies and procedures surrounding employee usage, supervisor review/approval, vendor payments, inventory of P-Cards, etc.; insecure access to P-Cards and inadequate P-Card monitoring; inability to identify duplicative payments for vendor invoices; 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.

Internal Audit Strategy

The objective of this review will be to determine whether internal controls in place are adequate surrounding the P-Card program. This audit will be designed to evaluate the adequacy of and compliance with policies and procedures regarding P-Card usage and monitoring. This includes assessing controls in regards to the physical and use security over P-Cards, as well as segregation of duties for approving, furnishing and reconciling P-Cards for accuracy. As part of this audit, we will review whether goods and services that are paid for were properly authorized, ordered and received in accordance with accounts payable and disbursement policies. Lastly, we will evaluate whether card holder setup and maintenance, monthly reconciliation and general monitoring of the program are functioning as designed.

RSM US LLP
7351 Office Park Place
Melbourne, Florida 32940-8229
(321) 751-6200
www.rsmus.com

RSM