

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA

Audit Plan and AU 260 Communication

For the fiscal year ended June 30, 2016



July 19, 2016

Table of Contents

Executive Summary	1
Communication	2
Auditor's Communication Responsibility	3
Additional Required Communications with the Audit and Budget Advisory Committee and Superintendent	4
Independence	5
The Concept of Materiality in Planning and Executing the Audit	6
Audit Team	7
Basic Users	8
Auditor's Responsibility Under <i>Government Auditing Standards</i> and Auditing Standards Generally Accepted in the United States of America	9
Management's Responsibilities	10
Deliverables	11
Engagement Timetable	12
Key Elements in Our Audit Methodology	13
Audit Approach	14 – 16
Areas of Emphasis and Significant Accounting Areas	17 – 23
Fraud Considerations and Risk of Management Override	24
Cybersecurity	25
Open Discussion	26

Executive Summary

This document outlines the audit planning process and communicates to The School Board of Miami-Dade County, Florida (the “School Board”) Audit and Budget Advisory Committee, the Superintendent, management, and members of the engagement team, the aspects of our preliminary approach and scope of services to be provided in conducting the audit of the basic financial statements of the School Board, as of and for the year ended June 30, 2016.

Communication

Effective communication between our Firm, the Superintendent, and the School Board is important to understanding matters related to the audit and in developing a constructive working relationship.

Your insights may assist us in understanding the School Board and its environment, in identifying appropriate sources of audit evidence, and in providing information about specific transactions or events. We will discuss with you your oversight of the effectiveness of internal control and any areas where you request additional procedures to be undertaken. We expect that you will timely communicate with us any matters you consider relevant to the audit. Such matters might include strategic decisions that may significantly affect the nature, timing, and extent of audit procedures, your suspicion or detection of fraud or abuse, or any concerns you may have about the integrity or competence of management.

Auditor's Communication Responsibility

We will timely communicate to you any fraud involving management and other fraud that causes a material misstatement of the financial statements, illegal acts, instances of noncompliance, or abuse that come to our attention (unless they are clearly inconsequential) and any disagreements with management and other serious difficulties encountered in performing the audit. We will also communicate to you and to management any significant deficiencies or material weaknesses in internal control that become known to us during the course of the audit. Other matters arising from the audit that are, in our professional judgment, significant and relevant to you in your oversight of the financial reporting process will be communicated to you in writing after the audit.

Additional Required Communications with the Audit and Budget Advisory Committee and Superintendent

Auditing Standard AU 260, *The Auditor's Communication With Those Charged With Governance*, require the auditor to provide certain information regarding the conduct of the audit to those who have responsibility for oversight of the financial reporting process. At the completion of the audit, the following matters will be communicated:

- Significant findings resulting from the audit
- The auditor's views about qualitative aspects of the School Board's significant accounting practices, including accounting policies, accounting estimates, and financial statement disclosures
- Significant difficulties, if any, encountered during the audit
- Uncorrected misstatements with management, other than those the auditor believe are not material
- Disagreements with management, if any
- Material misstatements that were brought to the attention of management as a result of audit procedures and corrected
- Management's consultations with other accountants
- Significant issues, if any, arising from the audit that were discussed, or the subject of correspondence with management
- Management's Representation Letter

Independence

Our independence policies and procedures are designed to provide reasonable assurance that our firm along with our SBE partners and all of our employees comply with applicable professional independence standards. Our policies address financial interest, business and family relationships, and non-audit services that may be thought to bear on our independence. For example, partners and professional employees of RSM US LLP; Anthony Brunson P.A; and Rodriguez, Trueba & Company P.A are restricted in their ability to own a direct financial interest or a material indirect financial interest in a client or any affiliates of a client. Also, if an immediate family member or close relative of a partner or professional employee is employed by a client in a key position, the incident must be reported and resolved in accordance with Firm policy. In addition, our policies restrict certain non-audit services that may be provided by RSM US LLP; Anthony Brunson P.A; and Rodriguez, Trueba & Company P.A, and require audit clients to accept certain responsibilities in connection with the provision of permitted non-attest services.

The Concept of Materiality in Planning and Executing the Audit

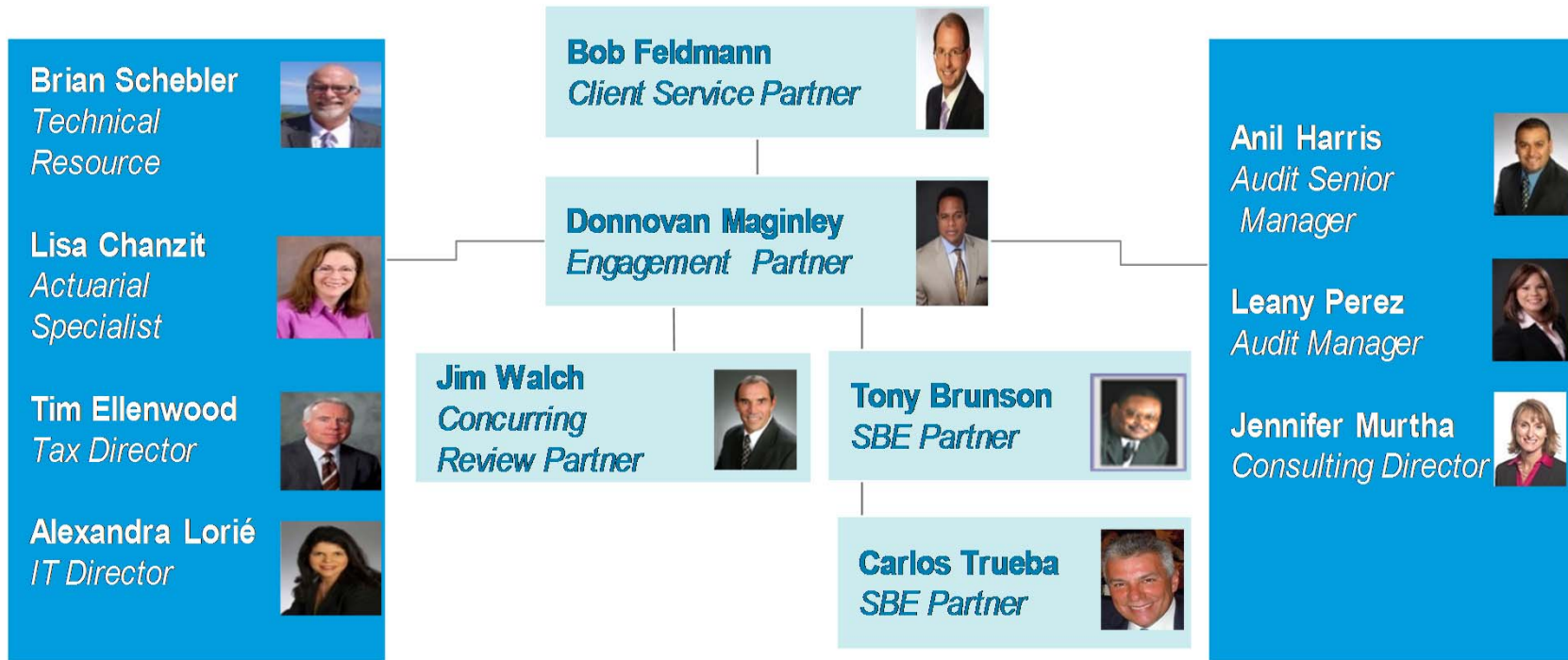
We apply the concept of materiality both in planning and performing the audit, evaluating the effect of identified misstatements on the audit, and the effect of uncorrected misstatements, if any, on the financial statements, and in forming the opinion in our report.

Our determination of materiality is a matter of professional judgment and is affected by our perception of the financial information needs of users of the financial statements. We establish performance materiality at an amount less than materiality for the financial statements as a whole to allow for the risk of misstatements that may not be detected by the audit. We use performance materiality for purposes of assessing the risks of material misstatement and determining the nature, timing and extent of further audit procedures.

Our assessment of materiality throughout the audit will be based on both quantitative and qualitative considerations. Because of the interaction of quantitative and qualitative considerations, misstatements of a relatively small amount could have a material effect on the current financial statements as well as financial statements of future periods. We will accumulate misstatements identified during the audit, other than those that are clearly immaterial. At the end of the audit, we will inform you of all individual unrecorded misstatements aggregated by us in connection with our evaluation of our audit test results.

Audit Team

The following is our organizational chart presenting all key personnel, including their titles and functions to be performed on this audit.



Basic Users

The audit is intended to serve the basic users as follows:

Users	Auditor
Citizens, Taxpayers, Bondholders, Federal and State Agencies	Issue an Independent Auditor's Opinion and other reports that provide reasonable assurance that the School Board's basic financial statement is fairly stated.
School Board Members and the Audit and Budget Advisory Committee	Assists the School Board members and the Audit and Budget Advisory Committee, through our work and reports, in discharging its corporate governance and compliance responsibilities.
Superintendent and Management	Provide observations and advice on financial reporting, accounting, and internal control and compliance matters. Share ideas and "best practices" from our experience.

Auditor's Responsibility Under *Government Auditing Standards* and Auditing Standards Generally Accepted in the United States of America

The primary objective of our audit is to express an opinion on the fair presentation of the basic financial statements of the School Board, in accordance with accounting principles generally accepted in the United States of America.

We have a responsibility to conduct our audit in accordance with auditing standards generally accepted in the United States of America, and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Furthermore, the audit will meet the requirements of *Florida Statutes, Rules of the Florida Auditor General, the U.S Office of Management and Budget Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations, and the Uniform Grant Guidance, as deemed applicable.*

In carrying out this responsibility, we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatements, whether caused by error or fraud. Because of the nature of audit evidence and the characteristics of fraud, we are to obtain reasonable, not absolute assurance that material misstatements are detected. We have no responsibility to obtain reasonable assurance that misstatements, whether caused by error or fraud, that are not material to the financial statements are detected.

Management's Responsibilities

As part of the audit process, management is responsible for the following:

- The preparation of the School Board's basic financial statements;
- Establishing and maintaining effective internal control over financial reporting and compliance;
- Identifying and ensuring that the School Board complies with the laws and regulations applicable to its activities;
- Making all financial records and related information available to the auditor;
- Providing assistance to the auditor in connection with the audit process;
- Providing the auditor with a letter that confirms certain representations made during the audit;
- Adjusting the basic financial statements to correct material misstatements and affirming to the auditor in the representation letter that the effects of any uncorrected misstatements aggregated by the auditor during the current engagement pertaining to the latest period presented are immaterial, both individually and in the aggregate, to the basic financial statements taken as whole; and
- Maintaining compliance with the provisions of grant agreements and other relevant contracts.

Deliverables

Planned deliverables to the School Board:

- Independent auditor's report on the School Board's basic financial statements;
- Management's representation letter;
- Management letters in accordance with the rules of the Auditor General of the State of Florida; and
- Audit and Budget Advisory Committee letter

**** The fiscal year 2016 single audit will be performed by the State Auditor General's Office**

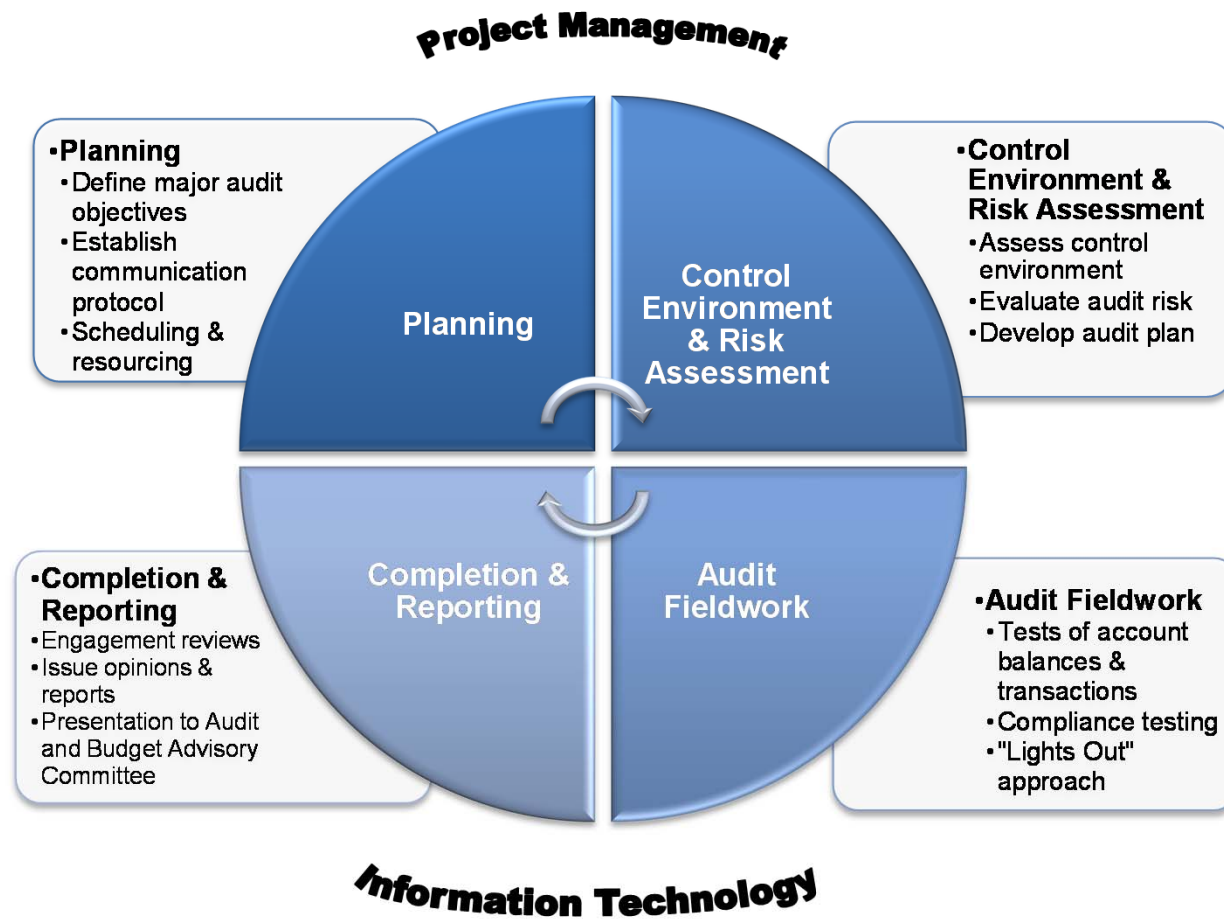
Engagement Timetable

The following chart depicts our proposed audit timeline for fiscal year 2016 which may be modified based on discussion with School Board staff during our audit planning meetings.

Audit Stage	July	Sept	Oct	Nov	Dec
Planning Phase:					
Present detailed audit plan to the Audit and Budget Advisory Committee	■				
Attend monthly Audit and Budget Advisory Committee meetings	■	■			■
Interim work	■	■			
Fieldwork Phase:					
Complete fieldwork		■	■	■	
Perform bi-weekly status meetings		■	■	■	
Reporting Phase:					
Exit conference				■	
Final reports				■	
Presentation to the Audit and Budget Advisory Committee:					■
Financial Statements					■
Management Letter and Single Audit Reports					■

Key Elements in Our Audit Methodology

The following diagram depicts an overview of our audit approach. Embedded within the approach is our overall project management as well as our utilization of information technology and computer-assisted audit techniques:



Audit Approach

Preliminary Phase

Planning Activities and Risk Assessment:

- Review interim financial information and prior year financial statements to identify accounting issues, if any;
- Review Board and Audit and Budget Advisory Committee minutes;
- Obtain copies of all new significant agreements, contracts, and pertinent documents, and evaluate the effects of new contracts on the scope of the audit;
- Review prior year compliance reports and management letter and obtain status updates from management;
- Highlight accounting and reporting matters and refine our understanding of audit risks;
- Meet with finance department personnel to coordinate schedules to be prepared; and
- Attend the School Board Audit and Budget Advisory Committee meetings to identify areas of concern and emphasis, fraud risk areas, new developments, planned operations, and strategic changes.

Audit Approach (continued)

Preliminary Phase (continued)

Planning Activities and Risk Assessment:

- Identify critical audit objectives;
- Obtain an understanding and document internal accounting control systems in place;
- Assess materiality considerations;
- Perform compliance tests of internal controls where appropriate;
- Identify substantive procedures to be performed;
- Coordinate IT audit testing of system files;
- Perform interim review of significant audit areas;
- Discuss interim findings and changes to our audit plan with management;
- Evaluate management's basis for developing estimates for reasonableness and consistency.

Audit Approach (continued)

Final Fieldwork and Reporting Phase

Fieldwork and Reporting:

- Confirm account balances
- Test account reconciliations
- Perform test of details
- Vouch significant transactions
- Perform substantive analytical procedures
- Evaluate third-party service organization reports
- Test and evaluate key estimates and management's key assumptions
- Perform compliance testing
- Draft independent auditor's report (CAFR)
- Draft single audit reports (when applicable)
- Draft management letter

Areas of Emphasis

Internal Controls

- Obtain and document our understanding of controls over key processes (cash receipts & disbursements, payroll, self-insurance, grant/program management, etc.)
- Document and determine testing procedures of IT general controls
- Review reports issued by the Office of Management and Compliance Audits

Estimates

- Budgets
- Self-insurance claims liability
- Compensated absences
- Litigation and other contingencies
- Retirement and other employee benefits

Routine Processes / Transactions

- Cash receipts and disbursements
- Revenues
- Payroll
- Purchases and accounts payables
- Property & equipment management
- Grant administration and compliance

Non-Routine Processes / Transactions

- Debt issuance and compliance with covenants
- Investments (portfolio management)
- Significant and unusual contracts
- Interlocal agreements

Significant Accounting Areas

Accounting Area	Risk	Audit Procedures
Self-insurance Claims Liability (\$179M*)	<ul style="list-style-type: none"> ▪ The School Board's self-insurance liability for general liability, employee health, workers' compensation, and general property and casualty is misstated ▪ Sufficient resources not available to satisfy outstanding claims ▪ Exposure to risk is not reflected in accrual estimate 	<ul style="list-style-type: none"> ▪ Review agreements and School Board Policy to ensure proper accrual ▪ Perform competence assessment of actuary ▪ Assess the propriety and completeness of data sent to actuary ▪ Evaluate actuarial reports and reasonableness of assumptions utilized ▪ Evaluate the amounts recorded compared to actuary's computation/estimates
Revenue (Taxes, Intergovernmental, etc.) (\$3.6B*)	<ul style="list-style-type: none"> ▪ Revenue is recognized improperly ▪ Unavailable/unearned revenue misstated 	<ul style="list-style-type: none"> ▪ Obtain an understanding of the School Board's revenue recognition policy and assess its compliance with GAAP ▪ Perform subsequent receipts/cut-off testing ▪ Confirm significant revenue balances
Capital Assets and Construction Activity (\$4.5B*)	<ul style="list-style-type: none"> ▪ Capital asset purchases not being capitalized ▪ Completed construction projects not being transferred to depreciable asset categories ▪ Impairment of capital assets not identified/ reported ▪ Depreciation not properly determined 	<ul style="list-style-type: none"> ▪ Test additions/deletions to capital assets ▪ Test depreciation expense ▪ Test completed projects and transfers ▪ Assess the applicability of GASB 51 - <i>Accounting and Financial Reporting for Intangible Assets</i>

* Prior year reported balance

Significant Accounting Areas (continued)

Accounting Area	Risk	Audit Procedures
Accounting for Retirement & Other Employee Benefits (\$8.6B*)	<ul style="list-style-type: none"> Amounts not properly estimated and recorded based on terms of agreements and School Board Policy 	<ul style="list-style-type: none"> Perform competence assessment of actuary Assess the propriety and completeness of data sent to and utilized by the actuary Evaluate actuarial reports and reasonableness of assumptions and models utilized Evaluate the amounts recorded compared to actuary's computation/estimates
Interfund Transfers (\$370M*)	<ul style="list-style-type: none"> Noncompliance with applicable laws, agreements, and School Board policy 	<ul style="list-style-type: none"> Test transfers to ensure compliance with applicable laws, agreements and School Board Policy Agree interfund transfers to annual adopted School Board budget
Fund Balance Accounting and GASB 54 - <i>Fund Balance Reporting and Governmental Fund Type Definitions</i> (\$453M*)	<ul style="list-style-type: none"> Equity transactions are not properly classified and/or presented in the appropriate categories Fund Balance policies and procedures are not properly defined 	<ul style="list-style-type: none"> Review minutes, statutes, debt indentures, and grant contracts to ascertain proper fund balance classification and reporting Review appropriate documentation to support fund balance designations Inquiry about the existence of restrictions and designations and ensure proper disclosure of such amounts

* Prior year reported balance

Significant Accounting Areas (continued)

Accounting Area	Risk	Audit Procedures
Cash and Investments (\$678M*)	<ul style="list-style-type: none"> Investments are not properly valued Investments and related income, gains and losses are not reported in the appropriate net position class Non-marketable investments lack adequate support for the valuation Investments purchased/held not in compliance with School Board Policy 	<ul style="list-style-type: none"> Perform test of internal control over treasury functions Test management's compliance with the School Board's investment policy Test investment valuations and review management's fair value assessment of those securities whose fair value is not readily determinable Confirm significant cash and investment balances
Liabilities and Expenditures (\$4.9B* and \$3.5B*, respectively*)	<ul style="list-style-type: none"> Liabilities and expenditures not reported in the proper period Possible budget violations 	<ul style="list-style-type: none"> Determine if there are any items in dispute at year end Review disbursements occurring subsequent to year end to test for unrecorded liabilities Obtain an explanation for significant variances in account balances occurring between fiscal years
Payroll Expenditures (\$1.8B*)	<ul style="list-style-type: none"> Improper payments to employees Liabilities and expenditures not reported in the proper period 	<ul style="list-style-type: none"> Perform internal control testing to assess whether there is proper supervisory review and approval of payroll transactions Test the accuracy and completeness of current year payroll balances

* Prior year reported balance

Significant Accounting Areas (continued)

Accounting Area	Risk	Audit Procedures
Accounting for Derivative Instruments and Hedge Activities (\$26.6M*)	<ul style="list-style-type: none"> Improper accounting/valuation of derivative instruments/transactions Improper financial statement presentation of derivative instruments/transactions 	<ul style="list-style-type: none"> Assess the accounting of derivative instruments and hedging activities Review agreements and assess the propriety of financial statement disclosures Evaluate specialists reports and reasonableness of assumptions utilized in valuing the instrument Perform competence assessment of specialists used Evaluate the effectiveness of the hedging instrument
Compliance with Bond Agreements (\$3.3B*)	<ul style="list-style-type: none"> Non-compliance with applicable bond agreement covenants Bond proceeds used for unallowed activity or costs 	<ul style="list-style-type: none"> Review bond agreement and test the School Board's compliances with applicable requirements/covenants Test expenditures funded with bond proceeds for compliance with bond agreements
Full Time Equivalent Determinations (FTE)	<ul style="list-style-type: none"> Amounts are not determined in accordance with Florida Department of Education Guidelines 	<ul style="list-style-type: none"> Review reports issued by the Office of Management and Compliance Audits regarding FTE audits Review Auditor General's most recent FTE Report

* Prior year reported balance

Significant Accounting Areas (continued)

Accounting Area	Risk	Audit Procedures
Results from Operations / Going Concern	<ul style="list-style-type: none"> ▪ Revenue does not equal or exceed expenditure ▪ Deteriorating financial condition 	<ul style="list-style-type: none"> ▪ Perform Financial Condition Assessment ▪ Review budget to actual statements
<p>Implementation of New Applicable Governmental Accounting Standards Board (GASB) Statements:</p> <ul style="list-style-type: none"> ▪ GASB Statement No. 72, <i>Fair Value Measurement and Application</i> ▪ GASB Statement No. 73, <i>Accounting and Financial Reporting for Pension and Related Assets That Are Not Within the Scope of GASB Statement No. 68, and Amendments to Certain Provisions of GASB Statement Nos. 67 and 68</i> 	<ul style="list-style-type: none"> ▪ Improper application and/or implementation of applicable GASB statements 	<ul style="list-style-type: none"> ▪ Assess proper application of fair value measurements to applicable account balances and the propriety of required fair value disclosures ▪ Assess the applicability and propriety of financial statement reporting of pension plans as required by GASB 73.

Significant Accounting Areas (continued)

Accounting Area	Risk	Audit Procedures
IT Systems	<ul style="list-style-type: none"> ▪ Unauthorized access – both from internal and external users ▪ Improper management of user access rights (assignment/monitoring) ▪ Improper use of portable devices to access the School Board's systems ▪ Improper change management system ▪ Program applications are not functioning as designed 	<ul style="list-style-type: none"> ▪ Test access controls ▪ Test change management system controls ▪ Test validity of program logic and configuration ▪ Test various interface systems and the financial reporting package ▪ Meet with IT Managers to discuss the impact of systems on financial reporting ▪ Project plan review ▪ System development life cycle assessment ▪ Test Payroll Certification Application

Fraud Considerations and Risk of Management Override

We are responsible for planning and performing the audit to obtain reasonable assurance about whether the financial statements are free of misstatement, whether caused by error or fraud (*SAS No. 99, Consideration of Fraud in a Financial Statement Audit*).

Our audit procedures will encompass requirements of SAS No. 99 which includes:

- Brainstorming among engagement team to identify fraud risk areas;
- Gathering information to facilitate the identification of and responses to fraud risk;
- Perform computer assisted testing of journal entries to identify significant and/or unusual transactions;
- Perform walkthroughs and test of controls to address the risk of management override of controls;
- Inquiry of various members of management and the Audit and Budget Advisory Committee their assessment of audit and fraud risk factors.

Cybersecurity

In January 2016, RSM US LLP published an article titled “**5 Cybersecurity Predictions for 2016**”. As organizations become increasingly reliant on technology to improve efficiency, productivity and mobility, vulnerabilities to cyberattacks are growing. While breaches at large organizations make headlines, no organization is too small to be a valuable target, and most companies will likely suffer a cybercrime at some point. Criminals and attack methods are evolving and becoming more sophisticated, so organizations and individuals must fully understand emerging threats and proactively plan to protect themselves.

Security and privacy advisors at RSM US LLP developed a list of five cybersecurity items that will likely emerge as significant threats to individuals and organizations in 2016.

We believe that this article, which is attached as Appendix A, will be of interest to you in your governance role as a member of the Audit and Budget Advisory Committee.



Open Discussion



RSM US LLP

801 Brickell Avenue Suite 801
Miami, Florida 33131
305.569.7986

www.rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM® and the RSM logo are registered trademarks of RSM International Association. *The power of being understood®* is a registered trademark of RSM US LLP.

© 2016 RSM US LLP. All Rights Reserved.



APPENDIX A

5 Cybersecurity Predictions for 2016



5 cybersecurity predictions for 2016

As cyberattacks become more frequent and sophisticated, RSM advisors discuss how to protect your organization against 2016's emerging cyberthreats.

INSIGHT ARTICLE | January 20, 2016

As companies become increasingly reliant on technology to improve efficiency, productivity and mobility, vulnerabilities to cyberattacks are growing. While breaches at large organizations make headlines, no organization is too small to be a valuable target, and most companies will likely suffer a cybercrime at some point. Criminals and attack methods are evolving and becoming more sophisticated, so organizations and individuals must fully understand emerging threats and proactively plan to protect themselves.

Security and privacy advisors at RSM US LLP, a national accounting, tax and consulting firm, have developed a list of five cybersecurity items that will likely emerge as significant threats to individuals and organizations in 2016. The five predictions are:

1. Cybercriminals will not just go after bits and pieces of data, as has been common practice in the past. Instead, cybercriminals will increasingly seek to build entire profiles from data collected and sell it as entire identities for monetization or for nation states to use for their targeted attacks.

AUTHORS

Loras Even
Principal

Travis Wendling
Sr. Associate

Shawn Jones
Sr. Associate

David Cossa
Sr. Associate

This means cybercriminals are no longer going after just credit cards, health care data or even personally identifiable information (PII). They are building a complete victim profile and then selling it to the highest bidder. A complete profile could include traditional information forms (bank account data, credit card data and health information), but also social media information, past residence addresses, dependent information and more.

This threat calls for increased controls necessary to protect traditionally stolen information, as well as safeguards consumers must take to ensure they do not provide too much information through social media. It also brings into question the publication of traditional public information such as property tax, permitting and other public records.

2. The “Internet of things” is still growing as seemingly everything (vehicles, appliances, children’s toys, safety systems and others) a business or consumer purchases is “Internet ready.” Unfortunately, we continue to read about these systems being broken into and either remotely controlled in disturbing ways or used to gather information on businesses or families without their knowledge.

In general, most of these systems have a portal hosted by the product’s manufacturer or provider, or one of their business partners, and have relatively weak authentication controls that require only a username and password. For example, the next time you see your Internet-connected intelligent thermostat adjust the temperature in your home, ask yourself if it changed the temperature because it was needed or did someone break into the portal account and now is experimenting with your thermostat?

Best practice security measures for the portals are to use similar security controls equivalent to online banking and credit card portals with multifactor authentication, forced password changes and account lockout.

3. Cybercriminals will continue to use social engineering to facilitate their system breach efforts. Postmortem breach reviews indicate that many successful breaches are dependent on attacking the organization's employees, customers or business partners through social engineering efforts.

People will likely be the weak link in security in the foreseeable future; and efforts to improve social engineering defenses must be implemented. Many organizations have security awareness programs and RSM advisors say they are slowly seeing improvement in the responses to their social engineering testing, but there is still room for improvement.

To improve security awareness, RSM advisors recommend conducting social engineering training and testing more than once a year, and then validating the effectiveness of the training through testing.

4. Health care information has more value per stolen record than most other forms of data theft (bank account, credit card, PII). Health care information is often tied to a social security number, and it is difficult to get a new number issued that does not tie back to the original number. It simply isn't as easy as getting a new credit card.

RSM advisors anticipate more breaches will occur in the health care industry in 2016, as more eligible professionals and hospitals move to electronic health record systems. As the industry continues this transition, an increase in hacking events will occur due to medical data being shared via electronic exchanges.

5. System security configuration issues continue to be a common source of security incidents and potential breaches. RSM continues to see too many weak security implementations for servers, workstations and other network devices during testing. New systems should be implemented using a National Institute of Standards and Technology (NIST) security reference or other guidelines to create a “base” image. That base image should then be used as a starting point when new systems are implemented.

A short list of common “wall of shame” security issues (practices not to do) follow:

- a. Using default administrative credentials. Most default credentials can be Googled.
- b. Improper administrator password usage. Many companies use the same local administrator password on all workstations and servers.
- c. Storing passwords insecurely. While conducting security testing for clients, RSM advisors find passwords on workstation shares, in text files, work documents and file names, and written on the side of monitors and keyboards.
- d. Running services on servers with administrative rights. If the service is compromised, the attacker would have administrative rights in the system.
- e. Weak passwords. Too often vendors use the same credentials on all of their customer systems.

All forms of data have value to cybercriminals, and hackers are using new methods and continually attempting to access sensitive information. Ignoring, or not properly addressing, security vulnerabilities can leave companies and individuals exposed to a breach with significant financial and reputational consequences. Understanding and addressing these emerging threats is critical to protecting your information, and reducing the potential for a data breach in the coming year.

THE POWER OF BEING UNDERSTOOD

AUDIT | TAX | CONSULTING

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

© 2016 RSM US LLP. All rights reserved.