COVID-19 and Internal Controls

Special Considerations for County Officials and Administrators
NYSAC thanks three+one for sponsoring the webinar today.

Garrett MacDonald
three+one
Internal Controls

• Why?
  – Mitigate Fraud Risk
  – Compliance
  – Accurate and Reliable Info
  – Effective & Efficient Information
  – Continue Operations

• Who?
  – Governance, Elected/Appointed Officials, Clerks, Support Staff… Everyone!

• How?
  – Adherence to the COSO Model
5 Components of COSO

- Control Environment
  - Integrity and Ethical Values
  - Governance Oversight and Independence from Management
  - Authority and Responsibilities, Reporting Lines
  - Commitment to Staffing & Employment Retention
  - Accountability
5 Components of COSO Cont’d

• Risk Assessment
  – Development of a Clear Concise Plan
  – Identify, Review, Analyze Risks
  – Consider Potential for Fraud
  – Assessing Changes and Impact
• What does this mean for the future?
5 Components of COSO Cont’d

• Control Activities
  – Develop, Document and Implement Activities that will Mitigate Risks
  – Develop, Document and Implement Control Activities Over Technology
  – Policies (expectations/requirements) and Procedures (execution)
5 Components of COSO Cont’d

• Information and Communication
  – Generate, Use, Share Accurate Info
  – Internal Communications
  – External Communications
5 Components of COSO Cont’d

• Monitoring Activities
  – Evaluation of Whether Internal Controls are Present and Operating Effectively
  – The Evaluation and Communication of Deficiencies
    – Corrective Action Plan
PRACTICAL EXAMPLE - OPERATING A MOTOR VEHICLE

Control Environment: NYS DMV, Courts

Control Activities: License Testing, Police

Information & Communication: Signage, Laws/Regulations, Tickets

Risk Assessment: Check Points, Cameras, Speed Traps

Monitoring: Point System, License Renewal, Probationary Periods
Action Plan

• Update and Document Risk Assessment (see Attachment 1)
  – Identify Objectives and Update
  – Identify Risks
  – Develop Response Plan
  – Monitor

• Evaluate segregation of duties
  – Authorization
  – Custody
  – Recording

• Check-in with IT (more to follow!)
Action Plan Cont’d

- Replace pen/paper with electronic files and email approvals
- Electronic Signatures & E-Stamps
- Reassign responsibilities as necessary
- Talk to your Team
  - Challenges?
  - What have they had to change?
  - What new responsibilities exist?
  - Where is the weakness(es)?
Evaluate the Future

- Identify and Train on New Tools
- Cross Training
- IT Capacity for Remote Working
- Evaluate “essential positions” vs. “remote positions”
- Document the “What If” and “Contingency Plans”
- Obtain Accounting Software Support where necessary
<table>
<thead>
<tr>
<th>Risk No.</th>
<th>Type of Risk</th>
<th>Description of Risk</th>
<th>Department</th>
<th>Significance of the Risk (score 1-10)</th>
<th>Resolution (Tolerate (1-2), Future Action (3-6), Immediate Action (7-10))</th>
<th>Correction Action Plan</th>
<th>Method for Monitoring (action item(s), frequency etc.)</th>
<th>Triggering Event for Resolution</th>
<th>Responsible Party</th>
<th>Corrective Action Plan Approved (Who, When)</th>
</tr>
</thead>
</table>
IT Risks in a Work From Home World

- What's Changed
- What's the Same
- What to Plan For
- What to do Now
- What to do Post Re-Entry
What’s Changed

• A Work From Home (WFH) Environment
  – Adds Complexity to the IT structure
  – Uncontrolled remote locations
  – Internet Access (VPN) and Bandwidth
  – Extends the user support past traditional boundaries
What’s Changed

• A Work From Home (WFH) Environment
  – Can add complexity to the data backup process
  – Potential for a larger cyber breach surface
  – Increases computer hygiene concerns
  – Adds data privacy complexity
  – Increases regulatory/data protection management surface
What’s the Same

• A WFH environment still requires everything you did before
  – Asset management
  – Software management
  – Risk management
  – Compliance with policies and procedures
  – Vendor Management
  – Security awareness training
  – Data backups
  – Program management
  – Regulatory Compliance
  – User Management and Accountability
  – …….
What to Plan For

• Resurgence in Regulatory Compliance
  – HIPAA
  – General Business Law 899-aa/899-bb
  – OSC Audit

• Risk Assessment Requirements
  – “Any material change….”

• Re-Entry WFH exceptions

• What your “new normal” will be
What to Do Now

- Poll all users for a current inventory of WFH equipment
- Access all WFH computers and assess hygiene state
- Assess “desktop” stored data
- Track VPN usage for unusual activity
What to Do Now

- Contact all “Cloud” vendors and confirm active user accounts
- Plan for GBL 899-aa/899-bb compliance
- Test your Computer Security Incident Response Plan (or draft one)
- Draft and publish asset return plan for re-entry
What to Do Post Re-Entry

• Asset track all incoming equipment

• Perform the Risk Assessment

• Perform a vulnerability scan on all returning computers

• Run comprehensive anti-virus and anti-malware scans on all computers
What to Do Post Re-Entry

• Contact “Cloud” vendors and re-certify active users
• Backup all data from all WFH computers
• Update Policy and Procedure suite with new processes for WFH controls
• Document any areas of concern for management review
Q&A
Thank You!