Internal Control in the Digital Age

Where did all the paper go?

Presented by: Scott Boren, C.H.A.E.
Independent Compliance Professional at Boren & Associates

In the beginning there was... PAPER!
Paper based control process:

- 1. Reports.
- 2. Registration cards
- 3. Credit card slips
- 4. Restaurant checks
- 5. Inventory counts and extention of value
- 6. Payroll and vendor checks

We had the ability to “touch and hold” the basic items that provided the basis for our control processes.
The Advantage was...

• 1. It was easily verifiable
• 2. Permanent
• 3. Indisputable

What were the risks ...

• 1. Financial misrepresentation.
• 2. Fraud
• 3. Theft

The risk was always an internal issue. Employees were always the primary perpetrators and the impact to the guest/client was minimal.

The exposure to the general public was not an issue.
The disadvantages were:

- A. Storage of all the paper.
- B. COST
- C. Permanent really isn’t PERMANENT. Aging paper fades, yellow, or molds. It just doesn’t really stand the test of time. Moreover, when you go to retrieve it, you have to put it back or it’s lost.

The man hours required for the mere maintenance of paper records (filing, storing, then moving and storing again) was always something of a “when we have time/slow period/free week”
Now we have...

The Digital Storage...

• 1. Convenient
• 2. Permanent
• 3. Cost effective
But the concern is...

• A. Capable of being Hacked
• B. Global
• C. Permanent

What should our control process be NOW!

• Internal control must now address a new threat.
  • - What do we store?
    • a. What is required by external auditor to document revenue and expense transactions.
    • b. What would be required by Taxing Authorities to back up exempt revenue.
    • c. What is required to document receivable transactions.
    • d. What would be necessary for regulating authorities (NLRB, Dept of Labor, Unemployment Comp).
    • e. What would be needed to document insurance claims in the event of loss.
What are the threats:

1. Employee’s still pose a threat for theft and misappropriation.
2. Hackers.
3. Natural disaster.
4. Legal challenges.

What should we be looking for:

A. Access control.
   - Password security
   - Terminated employee access
   - Firewalls
   - PCI compliance
   - Disaster Recovery standards
B. Financial Integrity.

• Inventory and purchasing systems are repriced with current values.
• OTA sites are monitored to maximize revenue.
• Adjustments are documented, approved and independently reviewed.
• Third Party payment sites (SERTFI, AUTHORIZE.NET) are recorded timely.
• Credit card refunds are done only when justified and only to the original card charged.
• Are systems backed up, stored to the cloud or a data recovery farm.

FINALLY...

• Operational Integrity
  • Are SOP's reviewed annually for relevance.
  • Are Operations, Human Resources AND Accounting members of the SOP committee.
  • Is there an independent reporting authority to report discrepancies to that can guarantee against reprisal.
Questions and Comments.

Contact Information:

- scottboren56@outlook.com
- Phone: 703-868-9017