INTERNAL CONTROLS OVER ELECTRONIC TRANSACTIONS

1. Why are internal controls important?
   - As a matter of obligation to the leaders of the organization – protect the assets, reputation, and people of the organization
   - Important to employees – to be protected from false accusation
   - Important to constituents – sound internal control promotes trust
   - Some organizations minimize the importance of internal control.
     - We’re too busy.
     - We’re too small.
       - Capacity or size concerns can be addressed by giving thought to making processes more efficient, using non-financial employees for certain roles, using volunteers where appropriate, etc.
     - We trust our employees.
       - We assume you trust your people – otherwise they shouldn’t be employees.
       - Maintaining sound internal control is not a practice based on mistrust.
     - Having sound internal control not only protects the organization’s assets, it also protects the reputations of those involved in administering the assets.

2. Today’s topic: Internal control over electronic transactions
   - Internal control processes and systems designed to reduce the risk that embezzlement or misappropriation could occur through electronic transactions and not be detected in a timely manner
   - Internal control comes in two primary forms:
     - Prevention controls – Designed to “keep something bad” from happening in the first place
     - Detection controls – Intended to identify an occurrence “after-the-fact”
   - Both are necessary in maintaining sound internal control.

3. Overarching principles for sound internal control
   - Dual control – Two or more people involved in the process
• **Segregation of duties** – Individuals responsible for asset custody are not also responsible for the related accounting and reporting

• **Appropriate oversight and monitoring** – Independent reviews of reconciliations, statements, reports, etc.

4. **Let’s talk about the details…**

• One process starting (or continuing) to gain traction:

• **Remote deposit capture (RDC)**
  
  ○ The ability to deposit a check into a bank account from a remote location, without having to physically deliver the check to the bank

  ▪ **Benefits**
    
    - Checks clear faster and funds are available sooner, which result in improved cash flow.
    
    - Later deposit cutoff times
    
    - Reduced costs
    
    - More convenient

  ▪ **Concerns**
    
    - Risk of scanning an item twice (Hint: immediately endorse the checks)
    
    - Security concerns between the time the check is processed and before it is destroyed (often 14 days)
    
    - **Data security measures** – the system contains sensitive personal information
    
    - Compliance with terms of agreement

  ○ **Internal controls**

    ▪ **Problem scenario**: One person is responsible for collecting and processing funds.
      
      - A risk of misappropriation is present (**with or without** RDC).
      
      - This is especially problematic if that person has accounting responsibilities over the funds.

    ▪ **Possible scheme**: skimming / stealing
Solution: Ensure adequate dual control

- Secure (processed and unprocessed) checks in a location or device requiring dual access.
- At least two people should remove the checks and be present during processing through the scanner.
- Endorse checks to prevent duplicate deposit (check scanning equipment may have this ability).
- Read the RDC service agreement...your banking institution may also have similar requirements written into the agreement.
- And remember!
  - Married persons or others with close personal relationships are considered “one” person when it comes to dual control.

Incoming ACH or credit card payments (including web-based transactions)

- What exactly is an ACH transaction?
  - Payments received and processed by the Automated Clearing House ("ACH"), an electronic network for financial transactions. ACH processes both credit and debit transactions.
  - Can occur in a variety of forms – web originated, personal account debit, telephone originated, conversion of checks into ACH transactions ("back office conversion"), and more.

- Benefits
  - Eliminates time spent processing manual payments
  - More secure than physical receipt if properly set up

- Concerns
  - Possible unauthorized use of bank accounts
  - Diverting funds to personal accounts
  - Issuing fictitious credits to merchant accounts

- Internal controls
  - Problem scenario: One person sets up accounts, downloads (or initiates) transactions, and reconciles accounts.
  - Possible scheme: Diverting funds to personal account
• **Solution!**
  - **Segregate duties**
    
    (a) Separate duty of initiating transactions from the accounting
    
    (b) Set up separate depository accounts for electronic commerce (makes it easier to monitor activity).
    
    (c) Make sure the person authorized under the merchant services agreement to make changes to the depository accounts has no accounting responsibilities.
    
    (d) Review credits issued to merchant account for propriety.
       
    Some systems will not allow a credit to a credit card number other than the one used to initiate the transaction and some systems will not allow credits that exceed prior charges to that account.
    
    (e) Do not share passwords.

• **What about electronic payments? (Wire/ACH)**

• **Problem scenario:** One person is responsible for initiating and authorizing electronic payments.
  
  o **Possible scheme:** Payments to self, vendors used personally, or shell companies

• **Solution!**
  
  o Implement **dual control** –
    
    ▪ No one person should be authorized to fully execute wire transfers or similar electronic disbursements alone.
  
  o **Segregate duties**
    
    ▪ The person(s) responsible for initiating or authorizing transactions should not be responsible for the related accounting. If your electronic disbursements system is built into your A/P process, the segregation of duties should be an aspect of user rights assigned.
    
  o **Also...**
    
    ▪ Restrict the ability to transfer funds from “non-operating” accounts outside the organization.
    
    ▪ Consider asking your bank to send an automatically generated email after each payment showing the amount and the recipient of the payment.
      
    - This email should be received by someone outside of the payables and accounting process.
• Have a knowledgeable person not directly involved in the disbursements process review the vendor list:
  - Review vendor name, address, invoice/payment history
  - Look for:
    (a) Multiple vendors with the similar names
    (b) Vendor addresses that appear to be personal home addresses
    (c) Multiple payments of the same dollar amount (especially round dollar amounts or amounts just below certain thresholds)
    (d) Significant payments to employees for other than normal travel-type reimbursements
    (e) Unfamiliar vendors (look up on the internet)

  • Generate a report of changes to vendor information (monthly or other appropriate interval).

  • Bank may offer an "ACH Fraud Filter" – automatically stops all ACH debits except those the customer specifically pre-authorizes.

• What is “positive pay”?
  
  o A service, offered by nearly every bank. Matches the account number, check number, and dollar amount of each check presented for payment against a list of checks previously authorized and issued by the organization.

  o Protects against altered checks and counterfeit checks

  o Items that do not match are not cleared...they are flagged and the organization is notified of the discrepancies.

  o Variation #1 – Payee validation and payee match
    
    • Same as positive pay, except the file also contains the payee’s name on the check
    • Should identify altered payee names

  o Variation #2 – “Reverse” positive pay
    
    • Checks presented for payment to the bank are provided to the customer.
    • The customer has the opportunity to review the checks presented for payment and determine if they should be paid or returned.
    • Cheaper than the other alternatives, generally less effective
- Always ensure that the process for preparing the check file and uploading it to the bank is secure and not subject to manipulation.

- What about online bill payment?
  - Reduces paper and is more environmentally friendly.
    AND
  - It saves time and costs over manual processes.
    - A recent article in The Wall Street Journal stated that a business check costs between $4 and $20 to fully prepare and process and that the cost of writing a check can be as much as five times the cost of an electronic payment.
  - It also streamlines the approval process.
    - Facilitates approvals and payment from people in multiple locations, including traveling.
  - Process generally involves scanning, faxing, or emailing bills to the payment processor. And then, automated processes take over - invoices are routed to pre-defined approvers.
  - The setup of the approval process is critical...want to ensure similar segregation of duties – the same person responsible for final approval of payment should not be the check preparer or accountant.
  - Some other benefits:
    - Easier to store and retrieve records
    - More secure than paper checks – bank account information is not making its way through the mail system
  - Some well-known service providers:
    - http://www.bill.com/
    - http://www.anybill.com/

- Electronic payroll processing
  - Problem scenario
    - One person is responsible for all phases of payroll processing, including maintaining personnel records, processing payroll details, and transmitting the direct deposit file to either employees or to the third-party payroll processor. No other parties closely review payroll reports.
  - Possible schemes
    - Fictitious employees
    - Manipulation of pay amounts
We’re evaluating potential service providers to help us with these processing areas.

What do we look for?

- Consider using service providers that can produce a “SOC 1” report.
- **SOC** = *Service Organization Controls*
  - Report on Controls at a Service Organization Relevant to User Entities’ Internal Control over Financial Reporting
    (a) Prepared in accordance with *Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization*
    (b) Specifically intended to meet the needs of the management of “user” entities (i.e. you) and the user entities’ auditors (i.e. us)
    (c) Evaluate the effect of the controls at the service organization on the user organizations’ financial statements
    (d) Therefore, they are considered a component of the users’ internal control...and are useful to auditors in planning and performing an audit.

- **Two** types of reports...
  - Type 2 (*preferred*) –
    (a) Report on the fairness of the presentation of management’s description of the service organization’s system and the suitability of the design and operating effectiveness of controls throughout a specified period
  - Type 1 (*good but not great*) –
    (a) Report on the fairness of the presentation of management’s description of the service organization’s system and the suitability of the design of the controls as of a specified date

- **Solution!**
  - **Segregate duties**
    - Do not have one person responsible for all aspects of payroll maintenance, preparation, and approvals.
    - The person responsible for executing direct deposit transactions should be separate from the person who prepares payroll and should review the payroll detail for propriety before submitting the file for direct deposit.
    - Payroll details should be reviewed by an appropriate (and independent) official for each payroll, in a controlled manner. (Direct receipt of reports, direct download of reports)
- So...Type 2 includes testing the operating effectiveness of the controls over a period of time. Type 1 does not...effectiveness of controls is generally tested based on a much smaller sample and is only “as of” a point in time.

- **Why** are they important?

- Rapid and sustained growth in businesses outsourcing various functions to service organizations, such as payroll processing companies, payment processors, cloud computing providers, etc.

- Growth of these organizations continued through the recession as companies faced pressure to improve efficiencies and reduce costs.

- Users submit (among other types of data) personal or confidential customer information to the service organization.

- Financial transactions...so real money is at risk!

- Responsibility over safeguarding that information remains with the user organization.

- SOC 1 audits are focused on financial reporting risks and controls (as specified by the service provider).

  (a) These are most applicable when the service provider performs financial transaction processing. Such as:

  i. Payroll processing

  ii. Transactional processing (e.g. credit card payments)

  iii. Asset management

- **What do we look for in the document?**

  - An unmodified (unqualified) opinion

  - Also pay attention to the stated control objectives, control activities, tests of operating effectiveness, and results of those tests.

  - A SOC 1 audit is not the same as being compliant with the Payment Card Industry Data Security Standard compliance (“PCI DSS”).

  - This is a set of requirements designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. (Regardless of size or number of transactions)

  - A SOC 1 audit is much, much more comprehensive.
What are some other things we should think about in this age of ever-increasing electronic transactions?

- Be sure to control access to systems...
  - It is very important to address propriety of system access rights.
  - Don't allow persons with accounting or custody responsibilities to also be the system administrator.
  - Make sure assigned rights are consistent with roles. Do not give access to areas that are not necessary to perform the job.
  - Never, ever share passwords with others.
    - Don't write down passwords.
    - Don't type passwords while others are watching.
    - Don't email passwords.
  - If the “other” person does something inappropriate, it is going to be difficult to defend your actions.
  - Consider changing passwords on a regular basis.
  - But...we are human...if you inadvertently (or purposefully!) share your password...don’t make a bad situation worse. Come clean, and get it changed!

Further...

- Immediately turn off all access for terminated employees
- Practice other sound internal control activities
  - Monitoring
    (a) Top-level official (or designee) [authorized signer] should receive the bank statements directly (unopened), review the bank statements and check images, and follow-up on unusual items.
    (b) Consider online review if physical review is not desired or practicable.
  - Independent (and timely) reconciliation of bank accounts
  - Review reconciliations and compare to balances in financial reports
- Consider documenting in a flowchart significant processing areas looking for holes or weaknesses.
  - Can assist new employees in understanding their roles
  - Can also assist management in reviewing processes for efficiency and proper controls
- Require vacation days and rotate duties occasionally.

**Emerging Areas**

- **Mobile giving**
  - Make giving as easy as buying from Amazon!
  - Studies indicate that 1 out of every 3 people in the U.S. use their mobile device as their primary tool to access the internet.
  - PayPal reports that globally, the total value of mobile donations in December 2012 was 242 percent larger than December 2011.
  - Giving by text which is billed straight to cell phone – no paperwork or forms to complete

- **Crowdfunding**
  - Many small “micro gifts”
  - Good for specific projects
  - Kickstarter, Indiegogo – popular crowdfunding platforms
  - Questions to ask:
    - What fees are charged?
    - Will the platform allow me to have the donors’ information?
    - How will they use that information? (What is their privacy policy?)
    - When will we receive the funds? (How many days later?)
    - What internal controls does the site provider maintain to ensure that we will receive all the funds we are supposed to receive?
    - Consider state charitable solicitation registration requirements.
Thank goodness. We made it! What now?

If you have the bases covered – congratulations! Continue to be vigilant.

If you believe your organization is vulnerable in any of the areas discussed previously...start by identifying specific risks.

- Develop specific controls to address the risks.
- Train and educate employees.
- Implement the new controls.
- Monitor...follow-up with staff regularly to make sure the controls are consistently applied.