Internal Control Update

Presenters: Dale Houser, Danny Johnson, & Steve Cardwell

1. Opening remarks

2. Overview of internal control

    a. Internal control comes in two primary forms (both are necessary in maintaining sound internal control):

        i. Prevention controls – designed to "keep something bad" from happening in the first place

        ii. Detection controls – intended to identify significant issues "after the fact"

    b. Fundamental concepts of sound internal control

        i. Segregation of duties

            1. Revenue: those involved in accounting for incoming funds should not also be involved in handling (or have the ability to access) those funds

            2. Accounts payable: those involved in processing accounts payable should not also be approvers

            3. In both transaction cycles, consider rotating individuals involved in the process from time to time (which is also helpful for cross-training purposes)

        ii. Dual control

            1. Revenue: having at least two unrelated individuals work together to process incoming funds

            2. Accounts payable: having at least two individuals involved in certain disbursement functions to release funds from the organization's bank account

        iii. Appropriate oversight/monitoring (independent review of reconciliations, statements, reports, etc.)

3. Electronic revenue collection

    a. There continues to be a proliferation of electronic revenue collection methods, which was further encouraged by the pandemic (organizations were forced to re-evaluate their physical collection processes and focus significantly on electronic revenue collection)

    b. A number of advantages

        i. Ease of collection

        ii. Available to donors 24/7/365

        iii. Facilitates recurring giving

iv. Timeliness and efficiency in funds processing

c. It is important to be vigilant and consider the internal controls over these processes

d. The following are some of the most common methods of electronic revenue collection

i. Online charitable giving and online payments for goods/services

1. Typically facilitated through a merchant service provider agreement

2. Allows for one-time or recurring payments

3. Allows for various payment methods (credit/debit cards, checking or other bank accounts, etc.)

ii. Online stock donations transmitted to a brokerage account

iii. Text-to-give

iv. PayPal, Venmo, and similar services

e. It is important to clearly and thoroughly communicate to donors and constituents the approved channels of electronic revenue collection for an Organization

i. We have heard of instances of scam websites, GoFundMe pages, or Facebook pages created to defraud donors using the name of legitimate nonprofit organizations

f. Controls and oversight activities

i. Employ proper controls over handling of sensitive donor information such as donor identity, credit/debit card account numbers, checking account numbers, address, etc.

ii. Obtain the most up-to-date written agreement with each merchant service provider

1. Verify the designated depository account and which individuals have the authority and ability to change the account

2. Maintain appropriate segregation of duties

a. Any individual authorized to change the depository account is separate from those who are processing or accounting for such funds (including access to modify donor records)

iii. Maintain controls to detect if an unauthorized change is made to the depository account, even for a short period of time

1. Many merchant service providers can alert numerous individuals within an organization to such changes, and restrict the frequency with which such

changes can be made. We encourage our clients to consider this with each of their merchant service providers.

iv. Independent audits of merchant service providers

1. When an organization utilizes a third-party service provider, the controls of the provider are, in effect, the controls of the Organization. This is not only limited to the electronic revenue collection process, but also to merchant service providers of cloud-based accounts payable management systems, general ledger systems, etc.

2. You should obtain independent assurance regarding the adequacy and effectiveness of the internal controls in place at any service provider it uses for significant financial processing areas

3. This is most commonly accomplished through a Service Organization Controls (SOC) report, which is an independent auditor's report designed to address the internal controls maintained by the service provider

a. There are three forms of SOC audits

i. SOC 1 (**preferred from the perspective of an Organization's external auditor**)

1. Focused on suitability of the design and operating effectiveness of controls at a merchant service provider

2. Involves determination of key identified control objectives and controls surrounding them

ii. SOC 2

1. Focused more broadly on availability, security, confidentiality, process integrity, and privacy of customer data

iii. SOC 3

1. Similar to SOC 2, but more generalized and high-level (meant for broader public consumption)

b. There are also two types of reports for SOC 1 and SOC 2 audits, cleverly named:

i. Type 1

1. Suitability of design of internal control as of a specific date

ii. Type 2

1. Suitability of design for a given period of time

2. More robust as compared to Type 1, requiring identification and testing of key identified control objectives. This is the preferred type, given the detailed testing required in this type.

c. It is highly recommended that an organization work with merchant service providers for transaction processing (revenue collection, bill pay, etc.) that have a clean SOC 1 Type 2 report

d. For cloud-based general ledger providers, a SOC 2 type 2 is most relevant and helpful for the external audit

e. Organizations should obtain and review a service provider's SOC report to ensure the service provider's controls are sound

f. If your Organization is utilizing or considering utilizing a merchant service provider that does not undergo a SOC audit, we would encourage you to take a closer look at that relationship and undergo your own due diligence assessment

g. Ultimately, organizations should employ these steps to have peace of mind and to avoid a potential misappropriation or diversion of funds

4. Electronic payment methods and practical internal control considerations

a. Wire transfers and ACH

i. How does it work?

ii. Internal control considerations

1. Does your organization maintain an agreement with your bank that requires two separate individuals to authorize any electronic disbursements (i.e., an initiator and approver)?

2. Are robust passwords maintained and not shared?

3. Is dual authentication utilized?

4. Are bank callbacks for transactions exceeding a predetermined dollar amount utilized?

5. Consider a debit block if available through your banking institution

a. How does it work?

b. Direct pay – web payment directly on the vendor's website

i. How does it work?

ii. Generally not recommended since it is difficult to control which individuals can set up or make these payments and what accounts they relate to (for example, an

employee can make a payment for their personal credit card on the American Express website)

iii. Internal control considerations

1. If you do have to make payments in this manner (though highly discouraged), we recommend implementing the following procedures to ensure that payments are only made to valid accounts. Without taking such steps, it would be difficult to know with certainty that the payment is made to a legitimate account (utilize a risk-based approach in consideration of your organization's risk tolerance)

a. Establish a predetermined dollar amount for which any payment over said amount requires a documented approval trail involving someone outside the day-to-day accounting function

b. An approving official should verify the validity of the routing account/payment information based on their review of the initiator's work – including a documented phone call to a known vendor phone number or through other independent verification means

c. The approving official's review should be documented with a brief narrative summarizing the review procedures performed, including contacting the appropriate vendor representative via a known phone number

c. Third-party payment processors (specifically, cloud-based accounts payable management systems)

i. How does it work?

ii. The benefits of a strong electronic bill pay application

1. Provides an opportunity to centralize disbursement activity

a. It becomes difficult to maintain proper controls over your organization's disbursement activity when using many methods to disburse funds (i.e., pay credit card and utilities through web payment; certain vendors are paid by check; other vendors are paid through ACH; etc.)

2. Provides a centralized location for all supporting documentation

3. Remote access to the system from anywhere and at any time (i.e., a real-time tracking system for disbursements)

4. Provides a secure environment with a detailed audit trail of approvals (denied transactions are required to go back through the approval sequence)

5. Most applications can facilitate the payment of bills both electronically and by check

a. Certain applications allow vendors to choose how they would like to be paid and change their payment information directly with a secure log-in feature (which can reduce the risk of spoofed emails leading your staff to change payment account information)

6. Eliminates the need to physically print and sign checks in a remote working environment

a. Eliminates the risk of misappropriation of a physical check (if it is lost, stolen, or modified after the fact)

b. <u>If you are still paying your bills by paper check and require actual sign-offs on checks, we would respectfully encourage you to find a strong cloud-based accounts payable management system</u>

7. Can segregate roles appropriately and be an overall superior internal control structure when set up correctly

iii. The overall advantages with respect to internal controls, bill approval, and bill payment efficiencies make electronic bill pay a worthy endeavor for any organization

1. Many organizations have greatly improved the efficiency of their bill-pay process through the use of such a system. Quality cloud-based accounts payable management systems are life-changing in their improvements to efficiency and can virtually eliminate the need for printing, signing, and mailing checks.

iv. There are several reputable applications available, such as BILL, SAP Concur, Emburse, etc. (these are not endorsements)

v. Internal control considerations

1. Consider if the application has a Service Organization Controls Report (i.e., a "SOC 1" report)

a. If your organization uses a service provider that does not have a SOC 1 Type 2 Report, how do you have comfort that a disbursement is appropriately remitted (i.e., the Service Organization made an error or failed to remit your funds to the intended party – whether intentionally or unintentionally)?

i. May be straightforward for vendor payments (i.e., the vendor would let you know they haven't been paid)

ii. What about other payments (grants, non-exchange transactions, etc.)?

b. If a service provider does not undergo a SOC 1 audit, the organization may need to consider alternative processors

2. Establish sound policies and procedures for reviews and approvals and build that structure into your cloud-based accounts payable management system

a. Are robust passwords maintained and not shared or is dual-authentication utilized?

b. It is important for an organization to establish proper roles within the cloud-based accounts payable management system to ensure that an appropriate segregation of duties is maintained. Careful thought needs to be given to all roles within the system, such as the following:

   i. What users are active in the system, and who can create new users?

   ii. What users can create or modify the approval sequence?

   iii. What users can initiate and process payments?

   iv. What users can create new vendors or modify a vendor's address or bank information?

      1. Certain cloud-based accounts payable management systems may allow you to set up controls that only allow vendors to update payment information directly (would require coordination and agreement with the vendor)

c. Roles in cloud-based accounts payable management systems that need to be considered and appropriately established generally consist of the following (though specific terminology may vary by application):

   i. Administrator (approve bills, authorize payments, schedule payments, manage users)

      1. The role of the software administrator in the general ledger and bill pay applications is critical

         a. Create new users and assign user rights

         b. Carefully evaluate which users can create or modify approval sequences

         c. Carefully evaluate which users can initiate and process payments

         d. Be sure other responsibilities align with the software administrator role (i.e., would not generally want someone who can authorize or edit transactions to be in this role)

         e. Understand each software application fully and the potential ability to edit transactions after the fact

      2. Generally, we recommend the administrator of all accounting software (including the general ledger, payroll, donor, and accounts payable management system) be held by an individual

outside the accounting function – we understand this is not always possible. In cases where it is not, we recommend:

a. Administrative rights be held by at least two individuals

b. All administrative rights, approval structure, change rights, etc., be established, reviewed, and locked down by these two individuals working together

c. Notifications established so each administrator is notified when any changes to rights or controls within the respective system are changed

d. Periodically obtain and review audit logs of changes to rights or controls within the respective system

ii. Accountant (processes bills, but does not approve payments)

iii. Clerk (enters bills only)

iv. Approver (reviews bills, approves bills, denies bills)

v. Payer (only able to pay bills [i.e., actually authorizes disbursement of funds])

vi. Auditor (view only – all account and transaction information is available, no edit rights or approval rights)

d. Ensure no single individual can push a payment through the system alone and it not be detected readily

e. Don't fall asleep at the switch when using cloud-based accounts payable management systems

i. It's still imperative that all of the policies and procedures in place regarding reviews, approvals, vendor changes, etc., are diligently followed for the system to continue to operate efficiently and effectively

d. Disbursements from other types of accounts

i. Know all of your accounts from which disbursements can be made

1. PayPal

a. Money can be freely moved out of a PayPal account, but it remains in the account until and unless it is moved. You need a good system for knowing when money goes into the account and for occasionally moving it out into other appropriate bank accounts.

2. Venmo

3. Virtual/digital currency

4. Investment accounts

    a. Someone outside of the accounting team should be regularly monitoring investment account activity for disbursements, and those disbursements should be verified for propriety

5. Any other bank accounts outside the regular accounting system

e. Credit card and expense reimbursements

    i. Review and approval of credit card transactions and expense reimbursements

        1. How to ensure that the process is sound and functioning well

            a. Receipts should be turned in timely

            b. Have the right people in the right roles

                i. Requires an awareness of and knowledge about the day-to-day activities of the department

                ii. Should include a detailed review of supporting documentation for expenditures

            c. Consider applications that help track approvals and documentation

                i. Ensure the administrator and other roles in such applications align with a proper segregation of duties

        2. Proper reviews and oversight can be tedious and seemingly a low-value exercise. However, it is a key function and responsibility, and must be done well to ensure transactions are legitimate.

f. Reviews and oversight

    i. Supporting documentation and approval

        1. Receipts should be turned in timely and reviewed in detail by an appropriate individual (an independent supervisor or equivalent)

    ii. Controlled review of bank activity

        1. What should be reviewed in this process?

            a. All forms of electronic disbursements (including transfers between accounts)

            b. Detail of batch disbursements from cloud-based accounts payable management system

2. Review should be properly documented – an important step in the audit trail

3. It's often the "last chance" you have to review a disbursement for propriety; once the month is closed and the bank account is reconciled, those transactions are often not revisited

5. Don't drop your guard: be prepared for the attack (email fraud scams)

   a. Phishing attempts

      i. Phishing emails are designed to get individuals to share sensitive financial information

      ii. Through monitoring email activity, bad actors can learn things about you or your activities with some research

   b. What to do to prevent becoming a victim of scams like this

      i. Be Vigilant – Verify Vendor Changes

      ii. Set up appropriate procedures for approving payment requests (consider schemes for changing vendor payment information or direct deposit bank accounts in the payroll process)

      iii. Disbursements should not be supported by email or similar instructions alone

         1. Verify the validity of the source of the request by calling the employee's or vendor's known phone number or by other independent means

         2. Once changes are verified directly with the vendor, require that an additional individual approve the change by confirming that verification with the vendor was performed and payment information was accurately updated

      iv. Maintain an agreement with your bank that requires two separate appropriately high-level people in your organization to authorize any wire transfers or similar disbursements

      v. Periodically review your organization's master vendor list (including payment information)

      vi. Evaluate the organization's level of insurance coverage in the areas of data security, cybersecurity liability, and theft.

   c. Bad things happen to good, smart people, and if you can implement some of these key principles, it may help you and your organization avoid significant pain and loss.