Updating Internal Controls for a Remote Environment

by Aaron Serna, Staff Associate II

Posted on May 21, 2020

A nonprofit organization (NPO) has a responsibility to its donors and other stakeholders to keep a strong internal control structure to help prevent and detect fraud. In the ever changing world we are in, it can become increasingly hard to ensure that our internal controls are still functioning even as our work environment changes.

The change that COVID-19 has created, although difficult, can be a trigger for many organizations to re-evaluate their existing controls. A great way to do this is to use the Committee of Sponsoring Organizations of the Treadway Commission framework (COSO framework). The COSO framework emerged in the 1980's as a joint initiative from many professional accounting organizations to combat corporate fraud. The framework sets the stage for an effective system of internal controls and is the foundation of many organizations' internal control structures.

The following are some items to consider when evaluating the effectiveness of a system of controls in accordance with the COSO framework.

Tone at the Top

Ensuring that the tone at the top remains focused on effective internal controls is critical to any system of controls. It can be especially crucial when employees' jobs undergo significant changes, such as those that could have occurred due to a global pandemic. Because the tone at the top tends to filter down to every employee, maintaining this level of

focus can help maintain employees' minds on operating within an effective internal control environment.

Assess Risk(s)

Management sets objectives to be completed and develops an internal control structure to meet them. Once developed, management should assess internal controls to mitigate risks of fraud or errors and ensure changes are made where necessary to mitigate those risks. While management should always be monitoring controls to improve them, any time there is a significant change to organizational operations, management should take the time to reevaluate its internal controls.

If the changes to operations occur suddenly, your organization may not have had the opportunity to reevaluate the impact on the control environment. The following are some key areas to consider:

- If you have manual review and authorization processes (e.g., requisition/PO review and approval, invoice review and approval, check signing, journal entry review and approval, time card signatures, etc.), have you considered the controls necessary to process these electronically and the risks associated with moving to an e-environment?
- What types of information technology (IT) security measures do you have in place if your workforce has moved to a part-time or full-time remote environment? Have you considered IT security measures for the remote networks used by your employees?
- Who has access to each key function of your financial reporting software? Does one person have access to all areas without a review process in place?
- How are you maintaining proper segregation of duties over the different functions (e.g., accounts payable, payroll, cash receipts, etc.) in a remote environment?

Determine and Implement a Plan to Address the Risk(s)

It is management's responsibility to ensure internal controls are in place to mitigate risks of fraud and error. Once management has assessed the risks, it needs to determine the best course of action to mitigate any identified risks. With a potential change to a partial or full remote working environment, or perhaps in a re-evaluation of operations that have remained unchanged, it will be necessary to design and implement a plan to address those risks.

The following are some ideas to aid in mitigating potential risks:

- Secondary and/or primary reviews can be completed in a remote environment. A review and sign off can be completed over email. There are also more sophisticated systems for maintaining and reviewing documents. Many financial systems have the ability to attach supporting documents for a specific transaction and allows for an electronic review and approval providing the specific user and date the document was approved. Researching your financial information system and its capabilities

can help increase efficiencies in your system of controls, while maintaining an appropriate review and approval process.

- IT security could be updated in simple and/or complex ways. A secured VPN can be provided so employees securely access an organization's financial information from a remote location. In addition, your organization could educate employees on phishing scams, other social engineering scams, or other methods used to hack or install malware or other vicious software into a company system. This education should be provided on an ongoing basis as new crises can create opportunities for new schemes.
- Additionally, your organization could evaluate existing IT policies, to ensure that they are up-to-date and reflect the current working environment. For example, every organization should maintain a current disaster recovery plan to ensure financial information is properly backed up and could be restored if necessary.
- Another crucial part of an IT controls policy is placing limits on employee access to unnecessary systems. Identifying which staff need to viewing and editing privileges within an organization-shared file room is a great place to start. A more in-depth look at your organization's financial software, payroll software, and other systems could help determine if system and function access has been sufficiently limited amongst your employees. For example, access in specific areas (e.g., accounts payable, cash receipting, bank reconciliations, journal entries and payroll) should be limited to only the employee(s) that need those capabilities. This can decrease the opportunities of fraud or error and allows for the segregation of duties within a remote environment similar to a physical environment.
- Lastly, it is very likely that the financial software you are using leaves a trail of changes that can be monitored. A periodic review of change logs is a great way to check that access and "privilege" controls are effective. Audit logs or similar reporting can help to determine who has completed what tasks and when, thus making it an effective tool for monitoring unusual activity.

The changing work environment has required many people to make adaptations to day-to-day life, and also has altered many organizations as we know them. As a result, organizations need to evaluate and change their internal controls accordingly. Although, the above is a small list of things to consider, with continued technology advancements and thought, management should be able to create and implement effective controls for a remote environment. If you are struggling with identifying certain risks or need suggestions on addressing them, please do not hesitate to contact us. We are here to help!