

Are your internal controls good enough?

Reprinted with permission from The Ohio Society of CPAs.

Given the current state of the economy, the potential for employee fraud is on the uptick. With employee layoffs on the rise, companies are more vulnerable to internal payment fraud because employees know where there are weaknesses in the organization's processes. Internal controls play a strong role in preventing fraud. This is a good time to review internal controls related to payments. Take this 20-question diagnostic challenge from the AICPA's Corporate Finance Insider to see if you can identify the potential landmines that can open your organization up to internal payment fraud.

This is a good time to review your internal controls related to payments. Take this 20-question diagnostic challenge and see if you can identify the potential landmines that can open your organization up to internal payment fraud.

1. Do you require all employees who have anything to do with the payment process to take at least five consecutive days of vacation? ___ Yes ___ No
2. Do you prohibit the ability to both approve invoices and enter invoice data? ___ Yes ___ No
3. Do you prevent one or more of your managers/executives from having access to all phases of the payment process, even though it might make training and managing more difficult? ___ Yes ___ No
4. Do you have a strong policy prohibiting the return of checks to requisitioners? ___ Yes ___ No
5. Are all changes made to the master vendor file periodically checked, no less frequently than once a month, but ideally every week?
___ Yes ___ No
6. Do you periodically (at least once a year) deactivate inactive accounts in your master vendor file? ___ Yes ___ No
7. Do you have an anonymous tip hotline? ___ Yes ___ No
8. Do you periodically check that your processors are not writing their passwords down where anyone can see them? ___ Yes ___ No
9. If you have a petty cash box, do you make sure that the location of the key is not common knowledge? ___ Yes ___ No
10. Do you wait until the end of the day to deliver checks to the mailroom for mailing? ___ Yes ___ No
11. Are unsigned checks always left in a secure location while waiting for signature — and not on someone's desk in an empty office?
___ Yes ___ No
12. Is the positive pay file uploaded only when checks are mailed?
___ Yes ___ No
13. Are checks only printed when they are going to be mailed — not earlier so they will reflect a date that matches your payment terms?
___ Yes ___ No
14. Are open receivers and POs always extinguished when an invoice is paid even if the invoice is paid outside accounts payable? ___ Yes ___ No
15. Is access to the master vendor file for entering vendors or changing vendor information severely limited?
___ Yes ___ No
16. When an employee making electronic payment transfers is terminated or leaves voluntarily, is the bank and p-card administrator immediately notified and passwords changed? ___ Yes ___ No
17. When a new vendor is to be entered into the master vendor file, do you require at least two signatures or approvals before adding them? ___ Yes ___ No
18. When a new vendor is to be entered into the master vendor file, do you do some checking to make sure the vendor is legitimate before adding them?
___ Yes ___ No
19. If you have a petty cash box, do you hold surprise audits and does everyone know you do that? ___ Yes ___ No
20. Do you have a written fraud policy, signed by a top-level executive, indicating zero tolerance for employee fraud? ___ Yes ___ No

The Answers

The preferred response, as most readers have probably concluded, to all the questions is yes. A negative response does not indicate fraud but rather that the controls surrounding that issue are weak and your organization is vulnerable. Nearly every organization will have at least a few areas that are less than perfect when it comes to internal controls. Look into them and determine if it is possible to tighten the controls or if you have to live with the weaker controls. If you cannot implement the best practices suggested here, regularly audit your problem areas.