40

Tips to Prevent and Detect Workplace Fraud

an E-book developed for you by:

CHORTEK
CPAs | BUSINESS ADVISORS

MILWAUKEE | CHICAGO | WASHINGTON, DC

Table of Contents

preventive controls

1. culture of ethics
2. free of moral hazards
3. risk management policy
4. required vacations
5. segregate duties
6. background and credit checks
7. limit access to records
8. payroll services and anti-fraud controls
9. fraud training programs
10. increase perception of detection
11. employee dishonesty insurance
12. assign unique user-profiles
13. implement separate passwords
14. develop secure electronic back-ups
15. limit corporate credit cards
16. financial lives of employees
17. establish zero-base budgets
18. mark invoices "paid"
19. terminate employee profiles
20. engage an anti-fraud specialist

detective controls

1. be accessible
2. analyze bank activities
3. anonymous tip line
4. examine cancelled checks
5. implement "proof of cash"
6. exclusive authority to approve
7. vendors and employee relationships
8. measure financial goals
9. scrutinize corporate credit card charges
10. competitive bids
11. receive payroll registers
12. reconcile cash receipts daily
13. audit internal accounting department
14. approve all journal entries
15. query the accounting system
16. re-assess business and financial risks
17. trend internal controls exceptions
18. review exit interview files
19. changes in customer payment patterns
20. physical count of inventory on hand

preventive controls

#1

Establish, communicate, and clearly reinforce a culture of ethics. Draft a written ethics policy and require employees to sign it annually.

#2

Ensure management is free of all moral hazards and is known for maintaining a zero-tolerance policy for moral infractions.

#3

Adopt a rigorous risk management policy with an eye toward identifying what could go wrong with the business in general and the accounting function in particular. Draft policies and procedures responsive to the risks you have identified and periodically test the efficacy of those policies and procedures.

#4

Require periodic vacations for those in a position to act contrary to their fiduciary duties and evaluate the ability of employees to cross-train in other practice areas.

#5

Segregate duties where possible such that no single individual has the ability to oversee a particular transaction from beginning to end. Separate the authority to enter into a transaction from the ability to account for it and the ability to physically possess the cash associated with it.

#6

Perform background AND credit checks for all employees working in sensitive business areas (particularly those related to cash).

#7

Physically limit access to records, facilities, software, assets, deposit slips, and check stock to those with a logical need for them.

#8

Where appropriate, make use of third party payroll services and banking anti-fraud controls (ie: deposit lockbox, positive pay files, electronic debit filters and transfer limits, secure key-tokens, read only access, etc…)

#9

Implement employee support and fraud training programs.

#10

Look for ways to increase the perception of detection on behalf of those in sensitive business areas. (ie: surveillance cameras and software, surprise internal / external audits, redundant controls, whistle-blower compensation, etc..)

#11

Purchase employee dishonesty insurance. Consider structuring the policy to cover frauds occurring over multiple years for total damages of at least $500,000. The policy should also contain provisions to pay for investigation and legal fees.

#12

Assign unique user-profiles in your accounting software and ensure the audit trail feature is turned on. Ensure "super-user" profile / "admin" login is not held by accounting personnel and available only to a single IT professional or other similar non-financial employee.

#13

Implement separate network and accounting software passwords. Passwords should be at least 6 digits long and consist of a random string of alpha-numeric characters with "special" characters ("?", "<", "+", "$", etc…) and be case specific. Passwords should be automatically retired after a period of time and "recycled" passwords should be precluded for at least five change cycles.

#14

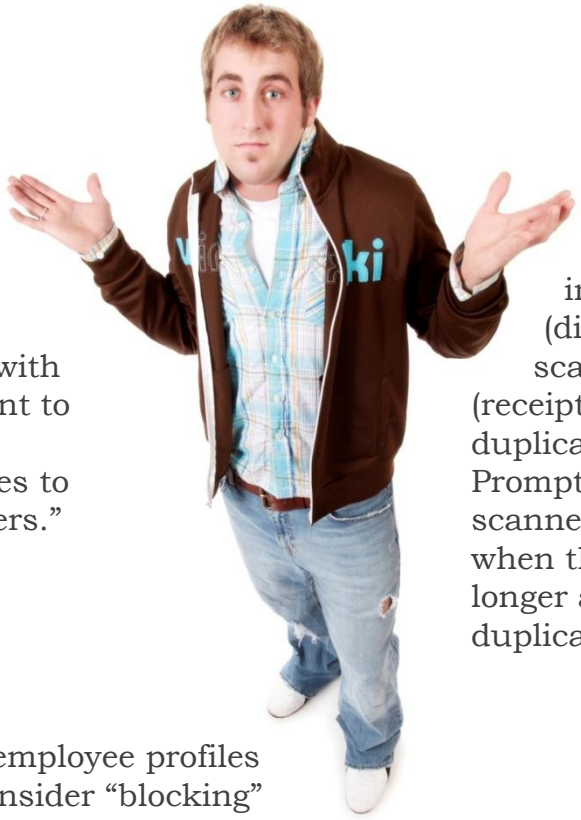
Develop and deploy secure electronic back-ups of the network files, accounting software data, and other key business files. Consider limiting the ability of accounting employees to save files directly to the workstation rather than the network.

#15

Limit corporate credit cards to a select group of non-accounting personnel and impose charge limits / filters on the cards. Require most employees to submit expense reports for corporate related charges.

#16

Be alert to changes in the financial lives of your employees (whether favorable or unfavorable) and assess whether any appear to be living beyond their means. Also be alert to those who are eager to reinforce your trust in them, habitually irritable, protective of their work-product, evasive, heavy handed in their relationships with others, dismissive of corporate policies, or the subject of significant life changes.



#17

Establish zero-base budgets and reasonable financial targets. Remember oppressive cultures with a zealous commitment to "meet the numbers" often tempt employees to "make up the numbers."

#18

Mark as "Paid" or "Deposited" all invoices (disbursements) and scanned checks (receipts) to prevent duplicate submission. Promptly dispose of scanned checks (receipts) when the software is no longer able to identify a duplicate submission.

#19

Promptly terminate employee profiles upon separation. Consider "blocking" customer, vendor, or bank accounts from posting access if unused for a period of time.

#20

Engage an anti-fraud specialist to periodically assist you in evaluating your fraud risks.

detective controls

#1

Be accessible to your employees, customers, and vendors. Implement robust upstream communication channels such as “open door” policies, surveys, and “town hall” meetings. Develop mechanisms to track customer and vendor correspondence / communications and preclude accounting personnel from coordinating those efforts.

#2

Bank reconciliation reviewers should receive bank statements and credit card statements directly from the source in unopened envelopes and scrutinize them for irregular items. If statements are not received, login to the bank website on a regular basis and analyze the activity for missing, unusual or unauthorized transactions.

#3

Implement an anonymous tip line.

#4

Examine cancelled checks for alterations for forged signatures.

#5

Review bank reconciliations in detail, paying particular attention to the nature and age of reconciling items. Consider implementing a “proof of cash” in lieu of bank reconciliations.

detective controls

#6

Senior non-accounting personnel should retain the exclusive authority to approve all disbursements and insist on inspecting original supporting documents before signing any checks. If exclusive authority is not feasible, implement counter-signatures for all checks in excess of a nominal amount. In general, signature stamps or other electronic signatures should not be used, unless they can be properly safeguarded and those applying such signatures do not have AP-related duties.

#7

Know your vendors and the relationships your staff has with them. Periodically compare the vendor and employee master files for similarities or other unusual features. When master file data are added, changed, or deleted, receive automated email alerts of the changes.

#8

Measure progress toward financial goals and investigate significant variances from expectations. Consider relating non-financial data to financial data and trend those relationships for unusual events or changes.

#9

Scrutinize corporate credit card charges and employee expense reimbursements. Classify and trend purchasing activity by expense and employee for unusual or excessive charges / reimbursements.

#10

Submit significant purchases to competitive bids or other market comparisons.

#11

Receive payroll registers directly from the payroll service prior to making them available to accounting personnel or distributing payroll. Scan the register for unauthorized pay increases, adjustments, bonuses, excessive hours, or other unusual items such as unknown employees. Relate the information on the register to personnel files or other expectations.

#12

Deposit and reconcile cash receipts on a daily basis.

#13

Conduct targeted internal audits of the accounting department on an unannounced basis.

#14

Review and approve all journal entries, debit / credit memo adjustments.

#15

Develop procedures to query the accounting system for check voids, duplicate payments, payments in excess of invoice amounts, or payments near approval thresholds.

detective controls

#16

Re-assess business and financial risks at least annually and relate those assessments to the internal controls you have.

#17

Develop procedures to capture, summarize, and trend internal control exceptions by employee for evidence of unidentified risks or inadequate risk assessments.

#18

Review exit interview files. When an exit interview provides the name and address of the subsequent employer, this information can be compared to vendor files and reveal potential conflicts of interest.

#19

Pay attention to changes in customer payment patterns. Sudden, unexplained variances in the amount of time a customer takes to pay should be investigated.

#20

Periodically, make a physical count of inventory on hand and compare this to the accounting records. Counts should be performed by those independent of the physical custody of inventory.

CHORTEK
CPAs | BUSINESS ADVISORS

Chortek is a forward thinking accounting and business advisory firm built on a team of knowledgeable professionals in accounting, audit, technology, forensic and litigation, and mergers and acquisitions who bring high value to clients' business and individual financial needs.

For over 65 years, Chortek has helped closely-held businesses obtain their financial goals in this competitive, global marketplace. Our entrepreneurial spirit and strong desire to see our clients' businesses grow drives our knowledgeable professionals to first listen to our clients' needs and then support their goals with meaningful and forward-thinking advice.

877.526.8227 | www.chortek.com/fraud

This Ebook was developed by: Paul Rodrigues, CPA, CFE, CFF, CGMA, MST, principal | prodrigues@chortek.com