Secure Nonfinancial Aspects

Be aware that larceny is not restricted to cash. Company managers must take extra care to secure other valuable commodities, including employee Social Security numbers, company credit card numbers, computer network access, and proprietary company plans, to name a few. In these areas, the key preventative is access. Only those with need-to-know authority should be privy to this critical information, or management leaves the company vulnerable to identity thieves, hackers, and industrial espionage.

All of these tips are easy to implement, are inexpensive, and will not create a huge demand for time. These tips are neither intrusive, nor unreasonable, and if you have not implemented these procedures, you must seriously consider doing so. They are absolutely critical to securing your company from within.

To find out more, contact:

Sean Brennan CPA, MBA
President
215.951.5585
sean@brennantax.com

Brennan and Company CPA, PC
5450 Germantown Avenue
Philadelphia, PA
215.951.5585

PICPA
Pennsylvania Institute of Certified Public Accountants

PICPA, with more than 21,000 members, advocates to strengthen the accounting profession and serve the public interest.

Produced in cooperation with the AICPA

7232/11

Secure from Within

Tips to help small business owners prevent internal fraud and theft

Nobody is immune to the threat of fraud. Not big companies. Not small companies. In fact, smaller enterprises may be more at risk to internal criminal activity because of a perceived familiarity among employees and an innate sense of trust by management.

Companies do not have to abandon trust in their employees, but they can take several useful actions that can protect them from internal fraud. If you want to curb abuses or the temptation to commit fraud, start with creating an ethical culture, institute basic fraud controls, and secure other nonfinancial aspects of your business.

Create an Ethical Culture

Company management establishes the level of integrity within their organization through their own actions. Only then can you insist on an ethical business environment for all. Some of the easier, yet effective, steps to implement are an official code of professional conduct, comprehensive ethics training, and an anonymous ethics hotline.

Code of Conduct – A code of professional conduct should clearly cover all the key behavior points, including areas such as use of corporate property, appropriate procurement procedures, and conflict of interest. Establishing clear rules will deter fraud by eliminating gray areas.

Ethics Training – Companies must hold training sessions that raise awareness of ethics issues and stress their importance. The training should focus on the practical application of the rules as it pertains to your company, and should be held at regular intervals.

Ethics Hotline – Give employees a way to confidentially report unethical behavior from within the ranks or to ask questions about an ethical dilemma.

Institute Fraud Controls

Once the parameters of an ethical business environment have been established, management can focus on fraud controls. Controls are systemic procedures, applicable to all, put in place as preventative measures. Below are five starter steps that can easily bolster your internal security:

Screen Potential Hires Thoroughly – Check past employment, references, and criminal records.

Separate Accounting Duties – Divide responsibilities so no one person controls all financial activity.

Review Bank Statements – Peruse statements before bookkeeping, looking for missing checks, checks to unknown parties, and checks written to third-parties but endorsed by an employee.

Surprise Audit – Hire a CPA to conduct an audit once a year, but at different times so the schedule is unpredictable.

Insist on Vacation – Mandate vacation time to be taken because those committing fraud often do not take vacation so they can guard their illicit activity.