Internal Controls for Businesses

According to fraud.net, insiders are responsible for around 22% of security incidents.

Insider fraud refers to activities committed within an organization by individuals who have access to sensitive information, systems, or resources as a result of their job function or position in the company. These individuals could be employees, contractors, vendors, or anyone else granted internal access. Insider fraud can involve illicit activities such as embezzlement, theft, data breaches, intellectual property theft, skimming, and more.

Signs of Employee Fraud

Identifying employee fraud can be difficult. However, many employees who steal from their employers do provide some red flags.

Employers should look out for employees:

- Living beyond their financial means
- Experiencing financial difficulties or family issues
- Working in positions to commit fraud
- Who frequently work late or longer hours than usual
- Who have an unusually close relationship with a vendor or supplier
- Who resist sharing their duties or oversight with other team members
- Experiencing a sudden changes in attitude, irritability, or defensiveness
- Creating a toxic work environment. This may actually be a cover for illegal activities

Employers should avoid engaging in discriminatory practices when identifying potential fraud.

Implementing Internal Controls can help Business Owners avoid Internal Fraud

1. Clearly define what constitutes fraud in your employee manual.
2. Conduct employee background checks.
3. Rotate job responsibilities to make it harder to hide fraudulent activities.
4. Distribute financial responsibilities among employees so one person doesn't have too much control over the organization's finances.
5. Set up an anonymous hotline and encourage employees to speak up if they suspect fraud.
6. Train employees to understand the risks of internal fraud.
7. Require employees to take time off without any system access.
8. Take advantage of free anti-fraud tools, like Positive Pay.
9. Limit writing paper checks and lock up your blank check stock.
10. Remain approachable so employees are comfortable taking extra time to verify calls, emails or texts requiring the transfer of funds.
11. Assign monthly bank reconciliations to someone who does not write checks.
12. Assign user permissions based on the lowest level required to do the job.
13. Don't ever share passwords. Ever.
14. Ensure your IT infrastructure is solid and complete updates as required.
15. Use financial system reports consistently to monitor crucial transactions like deleted invoices, credits, changes to disbursements.
16. Secure physical assets when not in use.
17. Implement a physical inventory count and reconcile it with your system records.
18. Verify vendor and client information. Ask for references to ensure they are legitimate.
19. Obtain an insurance policy that covers employee theft and fraud.