Selections from the Best Practices Archives

The Importance of Conducting an Annual Fraud Checkup

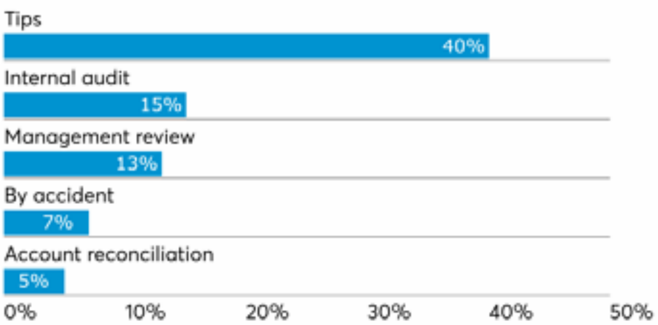
The Centers for Disease Control and Prevention recommend annual checkups for individuals of all ages. Why? Because "regular health exams and tests can help find problems before they start."

Not only is this true for our personal health, but also for the health of companies. When unchecked for too long, many companies unknowingly foster workplaces susceptible to fraud, which can cause devastating financial and reputational losses.

Vulnerability to fraud can pose a catastrophic risk to any company, but to a small business, it can mean life or death. Plagued by limited resources, small businesses are a ripe environment for employee misconduct.

Tips help catch fraudsters

The most common initial detection method for frauds



Source: 2018 ACFE Report to the Nations

The most cost-effective way to limit losses due to fraud is to prevent fraud from occurring. An annual fraud checkup is an excellent opportunity to not only test prevention measures, but also to identify vulnerabilities and implement additional anti-fraud controls before an exposure can turn into a full-blown case of fraud. A fraud checkup should include a collaboration of anti-fraud specialists and organizational leadership with extensive operational knowledge, such as internal audit or senior management.

The fraud checkup should include these topics:

Control environment

The foundation of an effective internal control system is the organization's control environment. The control environment — commonly called the "tone at the top" — includes management's philosophy, oversight and responsibilities, setting the tone of the organization and influencing the control consciousness of its people. Without an effective control environment, all other areas of internal control are likely to fail. They are only as good as the foundation upon which they are created.

- Are employees surveyed regarding their view of management's honesty and integrity?
- Are employees anonymously surveyed to assess morale?
- Has fraud prevention been incorporated into management's performance evaluation?
- Review performance goals. Are they realistic?
- Is there an established process for the oversight of fraud risks?

Stance on fraud — the perception of detection

The perception of detection is an important deterrent to fraud. That means putting employees and management on notice that all incidences of potential misconduct will be investigated.

- Is there a process in place for actively seeking out potential fraudulent conduct?
- Is the organization's stance on fraud clearly and regularly communicated?
- Does the organization have a code of conduct for employees based on the company's core values?
- Does the code of conduct identify how employees should seek advice when faced with ethical decisions?
- Is there a mechanism to anonymously report potential wrongdoing?

Employee education

Educating management and employees about fraud not only increases awareness, but also the likelihood that employees will become additional eyes and ears for the organization. Educational efforts should be positive and non-accusatory, with an emphasis that fraud, waste and abuse eventually cost everyone. Fraud education should be a part of employee orientation and annual training programs.

- Is fraud awareness training provided for departments, employees and managers?
- Do employees know what constitutes fraud?
- Does management communicate annually the importance of accountability and the organization's zero tolerance of fraudulent activity?

Conflict of interest statement

A conflict of interest occurs when an employee, manager or executive has an undisclosed economic or personal interest in a transaction that could hurt the organization. The most common situations that can give rise to a conflict of interest include accepting gifts from suppliers, employment by another organization, ownership of another company and close relationships with suppliers. The potential for a conflict of interest increases for employees in decision-making positions that would allow them to give preference to a vendor in exchange for anything of personal benefit to themselves, family or friends.

- Are employees required to complete an annual conflict of interest disclosure statement?
- Are employees provided a copy of the employee manual annually and required to sign a statement of acknowledgment and understanding?

Strengthening anti-fraud controls

Internal control plays an important role in fraud prevention. Although a system of weak internal controls does not mean that fraud exists, such a system can foster an environment for fraud to succeed. Conversely, a system of strong internal controls does not preclude fraud from occurring. However, such a system can help deter fraud and reduce the costs of any fraud that may occur.

Performing incompatible duties provides an easy opportunity for employees to commit fraud. For this reason, incompatible duties should be performed by different employees. For example, the responsibility for authorization, recording and custody of assets should never be assigned to just one person, because this person could commit fraud and more easily conceal it.

Segregation of duties can pose difficulties in departments with limited staff. Where there are too few employees to allow proper segregation of duties, direct oversight by management is one alternative to provide necessary control. In areas where it is difficult to add controls without compromising operational efficiency, analytical review and audit techniques such as data mining should be performed.

- Are duties properly segregated?
- Are physical safeguards in place?
- Are jobs rotated?
- Are vacations mandatory?

Independent checks

Independent checks test another employee's work. They include controls to assure the accuracy and completeness of the accounting records and often serve as an acceptable compensating control when segregation of duties is compromised.

- Are surprise audits performed?
- Is management review required for reconciliations, adjustments and write-offs?
- Does the internal audit function (if one exists) have adequate resources and authority to operate without undue influence from management?

Proactive fraud detection

According to the Association of Certified Fraud Examiners' 2018 Report to the Nations, 47 percent of all frauds detected are initially uncovered by a tip or by accident. This means that while internal audit, internal control and external audit all play an important role in the prevention and detection of fraud, they are simply not enough.

Proactive detection involves the deliberate search for misconduct, allowing transaction analysis close to the transaction date — helping to detect fraud sooner and more efficiently. A program designed to actively expose anomalies indicative of fraudulent activity should include the use of proactive data monitoring and data analysis. Combined with surprise audits, this trio of activities has been identified by the ACFE to be associated with a significant reduction in both fraud losses and duration.

- Is data mining software or continuous monitoring software used to detect fraud?
- Is a proactive audit approach utilized by the organization?
- Is artificial intelligence software used to identify risky transactions?

Measuring progress

An annual fraud checkup can provide a broad overview of the health of your organization's fraud prevention program. Conducted annually, the fraud checkup should give way to an ongoing fraud prevention plan. Review the findings of the fraud checkup with stakeholders and weigh the decision to implement additional anti-fraud controls with the organization's risk tolerance for the identified vulnerabilities.

(Source: AccountingToday - Audit & Accounting - Voices - March 25, 2019)

Cybersecurity Practices That Create the Best Remote Environment

As firms work remotely and cloud applications and security become more important than ever, accountants should be thinking about cybersecurity in new ways. As they say, the best defense is a good offense. But what may have worked in the past to protect you from hackers and other security threats is likely no longer sufficient as methods of attack become increasingly more sophisticated. There are, however, many cybersecurity strategies and controls that accounting firms can implement in order to significantly reduce the likelihood of a successful attack and minimize the resulting damage if attackers do gain access to systems. Here are some.

Password requirements

Passwords are the first line of defense against illegal access to systems and information. You need strict requirements for employee passwords that ensure length, complexity and randomness. A system wide requirement should also mandate that employees change their passwords at frequent intervals.

Multifactor authentication policy

Multifactor authentication is one of the best ways to prevent unauthorized access to email accounts and systems. A multifactor authentication policy requires a user to have two pieces of information to gain access, not only a password. This prevents attackers from gaining access even if user passwords or credentials have been compromised.

Role-based action control

Role-based access control is a neutral access policy that restricts every user's access rights solely on the basis of the role played in the organization, granting specific access to specific roles. Also known as a zero-trust model, this approach restructures access within your firm's systems based on a "never trust, always verify" philosophy targeted at preventing improper access.

Strong encryption at rest and in transit

Strong encryption is crucial to protecting your data from outside eyes, and you need to be sure that your data is secure regardless of where it is or how it's being used. Encryption must exist when data is at rest, or simply residing in your system, as well as when it's in transit, or moving from one location to another. Equally important is knowing who has access to the encryption keys at all times.

Patch management and regular vulnerability scanning

A crucial aspect of security is always knowing what systems are connected to your network and ensuring they are up to date. Regular vulnerability scanning will identify those systems for you, along with any potential vulnerabilities in them. Patch management pinpoints and installs any patches that are missing, confirming that your devices and systems always meet the most current security standards.

Network architecture and boundary protections

Preventing attacks requires understanding the structure of your systems and networks. Network architecture is the physical components of your technology stack and how they are configured, organized and interconnected. Boundary protections are processes for monitoring and controlling communications at the external boundaries of the network to prevent infiltration.

Audit logs

Spotting anomalies in networks and systems requires keeping detailed records of all activity. Audit logs are critical to collecting information on security incidents in order to analyze them, reverse-engineer the attack to identify vulnerabilities and determine whether changes are needed going forward.

Proactive security monitoring with AI behavior-based protection

Proactive security monitoring is crucial to detecting threats before they wreak havoc on your systems. Behavior-based security measures that incorporate advanced AI and machine learning are designed to proactively monitor all activities in order to identify anomalies and deviations from normal patterns and offer a protective response as soon as anything is detected.

Third-party audits and penetration tests

Cybersecurity threats aren't limited to your own systems. Most accounting firms work with several third-party vendors, including cloud providers, which offer alternate avenues of access to firm systems. Firms should regularly audit those third parties to ensure that their security measures meet firm standards, including running penetration tests to probe if the third party's defenses are sufficient to notice and prevent simulated attacks.

Backups and other resilience planning

If an attack happens, firms need to have a plan for recovering both data and applications. This requires having backups in place, but your strategy should go even further. IT resilience planning involves implementing tools and applications that will automatically take the necessary steps to protect your data and systems as soon as an issue arises, before backups are even necessary.

(Source: AccountingToday – Best of the Week – August 29, 2020)

How the Best Managers Identify and Develop Talent

Great managers are typically experts in their fields with a strong performance history and an interest in being in charge. But to lead effectively they need to develop another skill, one that is often overlooked: talent management.

The ability to see talent before others see it (internally and externally), unlock human potential, and find not just the best employee for each role, but also the best role for each employee, is crucial to running a topnotch team. In short, great managers are also great talent agents.

But becoming a great talent agent is not always easy. It requires us as leaders to be more open minded and to throw away outdated, albeit popular, hiring tactics. Too many of us look for talent in the same old (wrong) places, or follow the popular trend of thinking the "best hire" is the "best culture fit." These approaches undermine efforts to boost diversity (demographically and cognitively) and ultimately hinder creativity and innovation.

While there is no one "best" way to hire talent, there certainly are better approaches than those we have relied on in the past. After carefully scrutinizing the performance of what makes a competent and incompetent boss, here are seven science-based recommendations to help you update your hiring tactics, and develop your talent management skills along the way.

1) Think ahead.

Oddly, prospective employees are often asked during job interviews what their five-year career aspirations are or where they see themselves in five years; yet few managers ask themselves what their five-year talent strategy is. Most leaders know what kind of talent they are looking for in the moment, but far fewer think ahead to figure out whether or not their new hire has skills that align with their long-term strategy. If you know where you want to go, focus your efforts on hiring someone with the skills, abilities, and expertise you will need to move forward. Don't assume everyone you have today will stay. You must simultaneously play the long game while executing your shorter term goals.

2) Focus on the right traits.

The two biggest mistakes managers make when they evaluate other people's talents are: focusing too much on their past performance (even when they lack reliable metrics) and overrating the importance of their resume, hard skills, and technical expertise. The World Economic Forum predicts that 65% of today's jobs will no longer be around in 15 years. This means that leaders cannot place too much emphasis on the current educational curriculum, which is primarily designed to prepare people for present, rather than future, jobs. While we may not be able to guess what those jobs will be, it is clear that people will be more equipped to do them if they have certain soft skills, such as emotional intelligence, drive, and learnability. They are the foundational traits that determine new skill and knowledge acquisition. Moreover, these foundational aspects of talent are likely to become even more important with the rise of AI.

3) Don't go outside when you can stay inside.

Firms often hire externally when they could source better talent from within. Scientific reviews show that external hires will take longer to adapt and have higher rates of voluntary and involuntary exits — yet, they are generally paid more than internal candidates. That's why it's valuable to look for talent internally before you search outside your organization. Internal hires tend to have higher levels of adaptation and success rates than external hires, not least because they are better able to understand the culture and navigate the politics of the organization. They are also more likely to be loyal and committed to their company. Further, promoting internal candidates boosts other employees' engagement.

4) Think inclusively.

Most managers have a tendency to hire people who remind them of themselves. This tendency harms diversity and inhibits team performance. When we hire people just like us, we reduce the probability of creating teams with complementary skillsets, those with different and even opposite profiles. The only way to think about talent inclusively is to embrace people who are different from you and others already on your team. But we suggest you take it a step further and celebrate people who challenge traditional norms. The engine of progress is change, and change is unlikely to happen if you only hire people who perpetuate the status quo. We all know that companies with a diverse talent pipeline tend to have better financial results.

5) Be data-driven.
Every human — managers are no exception — makes bad decisions from time to time. But very few are interested in acknowledging this, which is why hiring biases are often so pervasive. In fact, research shows that hiring managers would rather inflate performance ratings than admit they hired the wrong person. Those of us in positions of power, therefore, need to be extra self-critical and test the outcomes of our decisions. For instance, when you hire someone, outline clear performance goals that can be easily evaluated by others, and see whether your view of their performance aligns with what others think and see. Likewise, before you nominate someone as a high-potential employee, arm yourself with solid data and evidence to ensure that your decision is fair and sensible, even if the future proves you wrong. Talent identification is an ongoing process of trial and error, and the point is not to get it right, but to find better ways of being wrong.

6) Think plural rather than singular.
We live in a world that often glorifies individualism and bemoans collectivity. However, almost everything of value that has ever been produced is the result of a collective human effort — people with different backgrounds coming together to turn their unique talents into a high performing synergy. Thus when you think about your talent pipeline, focus less on individuals and more on the configuration of your team: will people work together well, are they likely to complement each other, and do their functional and psychological roles align with what the team needs? On great teams, each individual is like an indispensable organ in charge of executing a specific function, making each part different from others, and the system greater than the sum of its units. Talent agents know that for teams to be successful, the individuals on them must embrace a "we before I" attitude.

7) Make people better.
Great managers recognize potential where others don't — and so do great talent agents. No matter how skilled your employees may be, you still need to help them grow in new ways. No matter how much an employee is struggling, you are responsible for attempting to help them find their footing. As professors Herminia Ibarra and Anne Scoular recently noted, "The role of the manager, in short, is becoming that of a coach." This means mastering the art of giving critical feedback, including the ability to have difficult conversations and address poor performance. It also means predicting your future talent needs so that you can stay ahead of the demand and have people on your team remain relevant, valuable assets for years to come. As our ManpowerGroup research surveying nearly 40,000 organizations across 43 countries shows, almost one in two employers report that they just cannot find the skills they need, which suggests that their talent planning strategies are not effective enough.

In sum, being a great manager is, in large part, about being an expert in talent matters. Fortunately, there is a well-established science of talent management, grounded on decades of industrial-organizational and management research. But unless you know how to apply it, this science is useless. And the most important part of this process is to never stop thinking about your employees' potential and talent. No other factor is likely to make such a big difference when it comes to building a high performing team.

(Source: AICPA – CPA Letter Daily - Harvard Business Review – January 14, 2020)