Fraud Prevention and Check-up

Are you vulnerable to fraud? Do you have adequate controls in place to prevent it? Test your company's fraud health with this free resource featuring a checklist and video.

Why you should take the Fraud Prevention Check-up

It is an affordable, easy-to-use way to identify gaps in your company's fraud prevention processed. By identifying risks early, you have a chance to fix the problem before losing money and becoming a victim of fraud.

It is a great opportunity to establish a relationship with a Certified Fraud Examiner (CFE) whom you can call when fraud questions arise. Since the risk of fraud can be reduced but it rarely eliminated, it is likely your company will experience fraud in the future and will need a CFE's assistance. A qualified CFE can help managers and its financial team develop and implement robust, relevant and effective controls to protect the company, its assets and reputation from emerging threats that current operating controls are not designed to address.

Strong fraud prevention processed bolster the confidence investors, regulators, audit committee members and the general public have in the integrity of your company's reports, which will help you attract and retain capital, enhance brand positioning and competitive advantage.

Fraud Check Up List

1. **Fraud risk oversight**
   To what extent has the organization established a process for oversight of fraud risks by the board of directors or others charged with governance (e.g., an audit committee)?

2. **Fraud risk ownership**
   To what extent has the organization created "ownership: of fraud risks by identifying a member of senior management as having responsibility for managing all fraud risks within the organization and by explicitly communicating to business unit managers that they are responsible for managing fraud risks within their area?

3. **Fraud risk assessment**
   To what extent has the organization implemented an ongoing process for regular identification of the significant fraud risks to which it is exposed?

4. **Fraud risk tolerance and risk management policy**
   To what extent has the organization identified and had approved by the board of directors its tolerance for different types of fraud risks? For example, some fraud risks may constitute a tolerable cost of doing business, while other may pose a catastrophic risk of financial or reputational damage.

   To what extent has the organization identified and had approved by the board of directors a policy on how it will manage its fraud risks? Such a policy should identify the risk owner responsible for managing fraud risks, what risks will be rejected (e.g., by declining certain business opportunities), what risks will be transferred to others through insurance or by contract, and what steps will be taken to manage the fraud risks that are retained.

5. **Process-level anti-fraud controls / reengineering**
   To what extent has the organization implemented measures to eliminate or reduce through process reengineering each of the significant fraud risks identified in its risk assessment? Basic controls include segregation of duties relating to authorization, custody if assets and recording or reporting of transactions. In some cases it may be more cost-effective to reengineer business processes to reduce fraud risks rather than layer on additional controls over existing processes. For example, some fraud risks relating to receipt of funds can be eliminated or greatly reduced by centralizing that function or outsourcing it to a banks lockbox processing facility, where stronger controls can be more affordable.

   To what extent has the organization implemented measures at the process level designed to prevent, deter and detect each of the significant fraud risks identified in its risk assessment? For example, the risk of sales representatives falsifying sales to earn sales commissions can be reduced through effective monitoring by their sales manager, with approval required for sales above a certain threshold.

6. **Environment-level anti-fraud controls**
   Major frauds usually involve senior members of management who are able to override process-level controls through their high level of authority. Preventing major frauds therefore requires a strong emphasis on creating a workplace environment that

promotes ethical behavior, deters wrongdoing and encourages all employees to communicate any known or suspected wrongdoing the appropriate person. Senior managers may be unable to perpetrate certain fraud schemes if employees decline to aid and abet them in committing a crime. Although "soft" controls to promote appropriate workplace behavior are more difficult to implement and evaluate than traditional "hard" controls, they appear to be the best defense against fraud involving senior management.

To what extent has the organization implemented a process to promote ethical behavior, deter wrongdoing and facilitate two-way communication on difficult issues? Such a process typically includes:

- Having a senior member of management who is responsible for the organization's processes to promote ethical behavior, deter wrongdoing and communicate appropriately on difficult issues. In large public companies, this may be a full-time position, such as ethics officer or compliance officer. In smaller companies, this will be an additional responsibility held by an existing member of management.

- A code of conduct for employees at all levels, based on the company's core values, which gives clear guidance on what behavior and actions are permitted and which ones are prohibited. The code should identify how employees should seek additional advice when faced with uncertain ethical decisions and how they should communicate concerns about known or potential wrongdoing.

- Training for all personnel upon hiring, and regularly thereafter, concerning the code of conduct, seeking advice and communicating potential wrongdoing.

- Communication systems to enable employees to seek advice where necessary prior to making a difficult ethical decisions and to express concern about known or potential wrongdoing. Advice systems may include an ethics or compliance telephone help line or email to an ethics or compliance office/officer. The same or similar systems may be used to enable employees (and sometimes vendors, customers and others) to communicate concerns about known or potential wrongdoing. Provision should be made to enable such communications to be made anonymously, though strenuous efforts should be made to create an environment in which callers feel sufficiently confident to express their concerns openly. Open communication makes it easier to resolve the issues raised, but protecting callers from retribution is an important concern.

- A process for promptly investigating (where appropriate) and resolving expressions of concern regarding known or potential-wrongdoing, then communicating the resolution to those who expressed the concern. The organization should have a plan that sets out what actions will be taken, and by whom, to investigate and resolve different types of concerns. Some issues will be best addressed by human resources personnel, some by general counsel, some by internal auditors and some may require investigation by fraud specialists. Having a prearranged plan will greatly speed and ease the response and will ensure appropriate persons are notified where potentially significant issues are involved (e.g., legal counsel, board of directors, audit committee, independent auditors, regulators, etc.)

- Monitoring of compliance with the code of conduct and participation in related training. Monitoring may include requiring at least annual confirmation of compliance and auditing of such confirmations to test their completeness and accuracy.
- Regular measurement of this extent to which the organization's ethics/compliance and fraud prevention goals are being achieved. Such measurement typically includes surveys of a statistically meaningful sample of employees. Surveys of employees' attitudes toward the company's ethics/compliance activities and the extent to which employees believe management acts in accordance with the code of conduct provide invaluable insight into how well those components are functioning
- Incorporation of ethics/compliance and fraud and fraud prevention goals into the performance measures against which managers are evaluated and which are used to determine performance-related compensation.

7. **Proactive fraud detection**

   To what extent has the organization established a process to detect, investigate and resolve potentially significant fraud? Such a process should typically include proactive fraud detection tests that are specifically designed to detect the potentially significant frauds identified in the organization's fraud risk assessment. Other measures can include audit "hooks" embedded in transaction processing systems that can flag suspicious transactions for investigation and/or approval prior to completion of processing. Leading-edge fraud detection methods include computerized email monitoring (where legally permitted) to identify use of certain phrases that might indicate planned or ongoing wrongdoing.

STEVEN A. MARTELLO MBA, JD, PhD is Managing Director and Chairman of Delta Security Services, Inc., a Global Security and Investigative solutions company, headquartered in New York, and offices in Long Island, NY, Juarez Mexico, and with strategic visibility throughout many areas of the world. Aside from managing global operations and counseling companies on mitigating threats to their people, information, brand, physical assets, IP and supply chain, as well as internal investigations, he shares his perspectives, experience and research on timely subject matter in the areas of security, investigations, risk mitigation, innovation, cutting edge management strategies, international business, emerging technological implications to the business process, discussion of disruptive technologies, and business modes, and threats to existing platforms, diplomatic and cultural protocol, cross cultural communication strategies, business strategy and process, and emerging opportunities for the 21st century economy.   He highlights a weekly blog on active and emerging threats, risks and scams targeted to business and individuals and how to effectively defeat them. For travel and safety tips, scams, and alerts, please visit our website at www.delta-ops.com