Who’s Minding the Store? Developing a Dynamic and Impactful Fraud Prevention Program

Presented by:

Bruce Dorris, Program Director, Association of Certified Fraud Examiners (ACFE)

Thursday, April 28, 2:00 - 3:15 p.m.
Who’s Minding the Store? Developing a Dynamic and Impactful Fraud Prevention Program

BRUCE DORRIS, J.D., CFE, CPA, CVA
Program Director
Association of Certified Fraud Examiners

2011 ECOA Sponsoring Partner Forum • San Antonio

2010 Report to the Nations on Occupational Fraud and Abuse

- The typical organization loses 5% of its annual revenues to fraud.
- The median loss due to occupational fraud was $160,000.
- Nearly one-quarter of frauds involved losses of at least $1 million.
Occupational frauds in our study were much more likely to be detected by a tip than through other means.

The typical fraudster is a first-time offender.

More than 85% of fraudsters in the study had never been previously charged or convicted for a fraud-related offense.

Fraud perpetrators often display warning signs that they are engaging in illicit activity.

- Living beyond means—43% of cases
- Financial difficulties—36% of cases

Anti-fraud controls appear to help reduce the cost and duration of occupational fraud schemes.
Integrating Fraud Prevention into Your Ethics and Compliance Program

- To manage risk of fraud, organizations should incorporate anti-fraud measures into their ethics and compliance programs.
- An integrated ethics, compliance, and anti-fraud program is not only a best practice, but makes good business sense as well.

Management should focus efforts and resources on:
- Conducting effective fraud risk assessments
- Enacting specific policies and internal controls specifically designed to prevent fraud
- Monitoring and assessing the effectiveness of the fraud prevention program
U.S. Sentencing Guidelines

- The U.S. Sentencing Guidelines encourage organizations to exercise due diligence in seeking to prevent and detect criminal conduct by their officers, directors, employees, and agents.
- They provide seven minimum elements that are required for due diligence.

1. Have policies defining standards and procedures to be followed by the organization’s agents and employees.
2. Assign specific high-level personnel who have ultimate responsibility to ensure compliance.
U.S. Sentencing Guidelines

3. Use due care not to delegate significant discretionary authority to people who the organization knew or should have known had a propensity to engage in illegal activities.

4. Communicate standards and procedures to all agents and employees and require participation in training programs.

5. Take reasonable steps to achieve compliance, for example, by use of monitoring and auditing systems and by having and publicizing a reporting system where employees can report criminal conduct without fear of retribution (hotline or ombudsman program).
6. Consistently enforce standards through appropriate discipline, ranging from dismissal to reprimand.

7. After detection of an offense, take all reasonable steps to appropriately respond to this offense and to prevent further similar offenses.

Sentencing Guidelines and COSO Internal Controls—Integrated Framework

- The requirements of the Sentencing Guidelines and COSO’s Internal Controls—Integrated Framework overlap significantly.
- Both focus on improving the entity’s control system.
- Companies should integrate their compliance efforts with their formal internal control initiatives.
<table>
<thead>
<tr>
<th>COMPONENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control Environment</strong></td>
</tr>
<tr>
<td>- Ethical tone at the top</td>
</tr>
<tr>
<td>- Organizational structure, including key areas of authority and responsibility</td>
</tr>
<tr>
<td>- Effective processes and controls—especially controls related to critical financial information</td>
</tr>
<tr>
<td>- Mechanism and support for employee reporting</td>
</tr>
<tr>
<td>- HR policies to ensure hiring and promotion of those who demonstrate integrity</td>
</tr>
<tr>
<td>- Consistent and appropriate discipline</td>
</tr>
</tbody>
</table>

| **Risk Assessment** |
| - Identification and analysis of risks related to operations, financial reporting, and compliance |
| - A strategy to manage risks |
| - Tailoring ethics and compliance programs to specifics of organization |
| - Development of compliance standards and procedures using risk assessment |
| - Periodic assessments of compliance and ethics risk |
| - Incentives to maintain internal controls |

| **Control Activities** |
| - Policies and procedures to help ensure that management's directives are followed |
| - Activities to ensure that fraud risks are addressed |
| - Standards and procedures capable of reducing the prospect of criminal conduct |
| - Identification of industry-specific compliance risks |

| **Information and Communication** |
| - Methods used to identify, capture, classify, and report pertinent information in an appropriate format and time frame |
| - Communication of roles and responsibilities pertaining to internal control |
| - Effective communication of standards and procedures to all employees and other agents |
| - Required participation in compliance and ethics training programs |

| **Monitoring** |
| - Ongoing assessment of the internal control system |
| - Ensures that internal controls are operating effectively |
| - Periodic evaluation of program effectiveness |
| - Identifies deficiencies in existing controls |
| - Responds to identified deficiencies by assessing the compliance program and making necessary modifications to prevent future problems |

What Makes a Good Fraud Risk Assessment?

- Used to monitor, change, or influence the factors that put the company at risk for fraud
- Serves as the foundation for the organization’s code of conduct, anti-fraud controls, and overall fraud prevention program

- An ineffective fraud risk assessment will result in deficiencies in the organization’s other anti-fraud initiatives
What Makes a Good Fraud Risk Assessment?

- Fits within the culture of the organization
- Sponsored and supported by the right people
- Encourages everyone to openly participate
- Generally embraced throughout the business as an important and valuable process

Key Elements of a Good Fraud Risk Assessment

- The right sponsor
- Collaborative effort of management and auditors
- Independence/objectivity of the assessment team
- Good working knowledge of the business
Key Elements of a Good Fraud Risk Assessment

- Access to people at all levels of the organization
- The ability to think the unthinkable
- A plan to keep the risk assessment alive and relevant

Fraud Prevention Controls

- *The perception of detection*—most effective prevention method
  - Management oversight
  - Reporting mechanisms
  - Whistleblower programs
  - Mandatory vacation and job rotation
  - Proactive audit policies
  - Surprise audits where possible
Fraud Prevention Controls

- **Zero tolerance**—no tolerance for fraud
- **Internal audit function**—employees must know they are actively and aggressively looking for fraud
- **Employee education**—need to know what constitutes fraud and how to recognize warning signs

Fraud Prevention Controls

- **Minimizing employee pressures**—assistance to employees facing problems and pressures
- **Code of conduct/ethics policy**—needs strong communication and support from management
  - Consider extending to vendors and agents
- **Fraud prevention policy**—separate, unambiguous written policy can be first step in fraud deterrence
Monitoring Your Fraud Prevention Program

- The performance of the overall program, as well as individual components, can be benchmarked:
  - Against management’s expected outcomes
  - Against prior trends in fraud prevention and occurrence
  - Against industry data and experiences (if available)
  - Across business units or functions

Conclusion

- Fraud is a risk that is always present, and it exists in every organization no matter what industry or size.
- It is important that ethics and compliance professionals adequately and proactively integrate fraud prevention as part of their organization’s compliance, ethics, and risk management process.
ECOA SPONSORING PARTNER FORUM
WHO’S MINDING THE STORE?
DEVELOPING A DYNAMIC AND IMPACTFUL
FRAUD PREVENTION PROGRAM
APRIL 28, 2011
SAN ANTONIO, TX

ACFE™
Association of Certified Fraud Examiners
D. BRUCE DORRIS, J.D., CFE, CPA, CVA
Program Director
Association of Certified Fraud Examiners
Austin, TX

Bruce Dorris is the Program Director for the ACFE since 2007 and is an advisory member to the ACFE Board of Regents. He earned his Juris Doctor from the Louisiana State University, Paul M. Hebert Law Center in 1993, and is licensed to practice law in state and federal courts in Texas and Louisiana.

Following a judicial clerkship after law school, Mr. Dorris was commissioned an Assistant District Attorney for the Caddo Parish District Attorney’s Office in Shreveport, Louisiana. He created and was the Director of its Financial Crimes Screening Section.

Mr. Dorris is also a licensed Certified Public Accountant, primarily in business valuation and litigation support practices, and also holds the designation of Certified Valuation Analyst. He was an Adjunct Instructor in the Accounting and Business Law Department of Louisiana State University in Shreveport, and has taught with the Becker CPA Review Program.

He is a Past President in the Louisiana District Attorneys’ Association, and has worked in the Louisiana House of Representatives Fiscal Division. He has testified numerous times before legislative committees and was a frequent lecturer with prosecutor and accountant training associations. He formerly served on the Board of Directors with the National White Collar Crime Center, and was the Vice Chairman of its Audit Committee.

Bruce Dorris is a member of the Association of Certified Fraud Examiners, the Louisiana State Bar Association, the Texas State Bar Association, the American Bar Association, the American Institute of Certified Public Accountants, and the National Association of Certified Valuation Analysts.
# TABLE OF CONTENTS

**WHO’S MINDING THE STORE? DEVELOPING A DYNAMIC AND IMPACTFUL FRAUD PREVENTION PROGRAM**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Impact of Fraud on Organizations</td>
<td>1</td>
</tr>
<tr>
<td>Integrating Fraud Prevention into Your Ethics and Compliance Program</td>
<td>2</td>
</tr>
<tr>
<td>What Makes a Good Fraud Risk Assessment?</td>
<td>5</td>
</tr>
<tr>
<td>Fraud Preventive Controls</td>
<td>9</td>
</tr>
<tr>
<td>Monitoring Your Fraud Prevention Program</td>
<td>16</td>
</tr>
<tr>
<td>Conclusion</td>
<td>16</td>
</tr>
</tbody>
</table>
DEVELOPING A DYNAMIC AND IMPACTFUL FRAUD PREVENTION PROGRAM

The Impact of Fraud on Organizations

*All Organizations Are Susceptible to Fraud*

Fraud is an uncomfortable risk to address. Most directors, executives, and managers would much rather believe that their organization’s employees would never steal from the company. However, it is actually those companies that are the least attentive to the potential for fraud that are at the most risk.

The truth is that fraud occurs in all organizations, of every size, in every industry, and in every city. No entity is immune. The fundamental reason for this is that fraud is a human problem, not an accounting problem. As long as organizations are employing individuals to perform the business functions, the risk for fraud exists. Only by recognizing the risk of fraud, and taking steps to proactively and continually address it, can organizations mitigate the potentially devastating impact of white-collar crime.

*The Shocking Cost of Fraud*

The ACFE’s 2010 Report to the Nations on Occupational Fraud and Abuse, an analysis of 1,843 fraud cases investigated by anti-fraud professionals around the world, reports that organizations lose an estimated 5% of their annual revenues to occupational fraud. Other significant findings include the following:

- The median loss caused by the occupational fraud cases in the study was $160,000. Nearly one-quarter of the frauds involved losses of at least $1 million.
- Occupational frauds are much more likely to be detected by tip than by any other means.
- The typical fraudster is a first-time offender. More than 85% of fraudsters in the study had never been previously charged or convicted for a fraud-related
offense. This finding is consistent with prior ACFE studies.

- Fraud perpetrators often display warning signs that they are engaging in illicit activity. The most common behavioral red flags displayed by the perpetrators were living beyond their means (43% of cases) and experiencing financial difficulties (36% of cases).
- Anti-fraud controls appear to help reduce the cost and duration of occupational fraud schemes. The Report looks at the effect of 15 common controls on the median loss and duration of the frauds. Victim organizations that had these controls in place had significantly lower losses and time-to-detection than organizations without the controls.

**Integrating Fraud Prevention into Your Ethics and Compliance Program**

The need to manage the risk of fraud is clear. Incorporating anti-fraud measures into the organization’s ethics and compliance program is not only a best practice, it makes good business sense as well. Specifically, organizations need to focus their efforts and resources on:

- Conducting effective fraud risk assessments
- Enacting specific policies and internal controls specifically designed to prevent fraud
- Monitoring and assessing the effectiveness of the fraud prevention program

**Corporate Sentencing Guidelines**

The U.S. Corporate Sentencing Guidelines encourage organizations to exercise due diligence in seeking to prevent and detect criminal conduct by their officers, directors, employees, and agents. The following seven minimum elements are required by the Sentencing Guidelines for due diligence:
### DEVELOPING A DYNAMIC AND IMPACTFUL FRAUD PREVENTION PROGRAM

1. Have policies defining standards and procedures to be followed by the organization’s agents and employees.
2. Assign specific high-level personnel who have ultimate responsibility to ensure compliance.
3. Use due care not to delegate significant discretionary authority to people who the organization knew or should have known had a propensity to engage in illegal activities.
4. Communicate standards and procedures to all agents and employees and require participation in training programs.
5. Take reasonable steps to achieve compliance, for example, by use of monitoring and auditing systems and by having and publicizing a reporting system where employees can report criminal conduct without fear of retribution.
6. Consistently enforce standards through appropriate discipline, ranging from dismissal to reprimand.
7. After detection of an offense, take all reasonable steps to appropriately respond to this offense and to prevent further similar offenses—including modifying its program and appropriately disciplining individuals who were responsible for the offense and those who failed to detect it.

### Comparison of Sentencing Guidelines and COSO Internal Control—Integrated Framework

The requirements of the Corporate Sentencing Guidelines overlap significantly with the suggested components of COSO’s Internal Control—Integrated Framework. Both focus on improving the entity’s control system. The following chart examines the relationship between the two and illustrates how companies can integrate their compliance efforts with their formal internal control initiatives.
<table>
<thead>
<tr>
<th>COMPONENTS</th>
<th>COSO INTERNAL CONTROL—INTEGRATED FRAMEWORK</th>
<th>SENTENCING GUIDELINES</th>
</tr>
</thead>
</table>
| Control Environment        | • Ethical tone at the top  
• Organizational structure, including key areas of authority and reporting lines  
• Policies—both formal and informal—to reward ethical conduct and punish unethical actions  
• Mechanism and support for employee reporting  
• HR policies to ensure hiring and promotion of those who demonstrate integrity  
• Consistent and appropriate discipline | • Code of conduct  
• Promote a culture that encourages ethical conduct and compliance  
• Knowledgeable governing authority with reasonable oversight  
• High-level personnel assigned overall responsibility for the program  
• Incentives to promote proper conduct and discourage improper conduct  
• Reporting mechanisms for employees and agents  
• Prohibit retaliation against those who make good faith reports of suspected violations  
• Due diligence to avoid delegation of authority to those with criminal tendencies  
• Consistent and appropriate discipline |
| Risk Assessment            | • Identification and analysis of risks related to operations, financial reporting, and compliance  
• A strategy to manage risks  
• Tailoring ethics and compliance programs to specifics of organization | • Develop compliance standards and procedures using risk assessment  
• Periodic assessments of compliance and ethics risk  
• Incentives to maintain internal controls  
• Identification of industry-specific compliance risks |
| Control Activities         | • Policies and procedures to help ensure that management’s directives are followed  
• Activities to ensure fraud risks are addressed | • Standards and procedures capable of reducing the prospect of criminal conduct  
• Determination of modifications needed to prevent future problems |
| Information and Communication | • Methods used to identify, capture, classify, and report pertinent information in an appropriate format and time frame  
• Communication of roles and responsibilities pertaining to internal control | • Effective communication of standards and procedures to all employees and other agents  
• Required participation in compliance and ethics training programs  
• Compliance and ethics training and communications that are ongoing, updated, and appropriate to each group of employees |
| Monitoring                 | • Ongoing assessment of the internal control system  
• Actions to correct and remediate any deficiencies | • Use of monitoring and auditing systems designed to detect criminal conduct  
• Periodic evaluation of program effectiveness  
• After discovering misconduct, take reasonable steps to remedy the harm caused (e.g., provide restitution to victims and self-reporting and cooperation with authorities)  
• Respond to identified offenses by assessing the compliance program and making necessary modifications to prevent future problems |
What Makes a Good Fraud Risk Assessment?

A fraud risk assessment is effective only if the organization embraces it and uses the results to monitor, change, or influence the factors that put the company at risk for fraud. The fraud risk assessment should serve as the foundation for the organization’s code of conduct, anti-fraud controls, and overall fraud prevention program. Accordingly, an ineffective fraud risk assessment will result in deficiencies in the organization’s other anti-fraud initiatives.

A good fraud risk assessment is one that fits within the culture of the organization, is sponsored and supported by the right people, encourages everyone to openly participate, and is generally embraced throughout the business as an important and valuable process.

There are several key elements to conducting a good fraud risk assessment:

- The right sponsor
- Collaborative effort of management and auditors
- Independence/objectivity of the people leading and conducting the work
- A good working knowledge of the business
- Access to people at all levels of the organization
- The ability to think the unthinkable
- A plan to keep it alive and relevant

**The Right Sponsor**

Having the right sponsor for a fraud risk assessment is extremely important in ensuring its success and effectiveness. The sponsor must be senior enough in the organization to command the respect of the employees and elicit full cooperation in the process. The sponsor also must be someone who is committed to learning the truth about where the company’s fraud vulnerabilities are; he must be a truth seeker—not someone who is
prone to rationalization or denial. In the ideal situation, the sponsor would be an independent board director or audit committee member; however, a chief executive officer or other internal senior leader can be equally as effective.

Organizational culture plays a key role in influencing the organization’s vulnerability to fraud. If the company’s culture is shaped by a strong and domineering leader, obtaining candid participation from the people in the business might be difficult with that leader as sponsor of the fraud risk assessment.

**Collaborative Effort of Management and Auditors**

As regulations and professional standards indicate, both management and auditors have a responsibility for fraud risk management. However, each of these parties has unique knowledge and perspective of the fraud risks faced by the organization.

Management has intricate familiarity with business operations; responsibility for assessing business risks and implementing organizational controls; authority to adjust operations; influence over the organization's culture and ethical atmosphere; and control over the organization’s resources (e.g., people and systems).

Auditors, conversely, are trained in risk identification and assessment, and have an expertise in evaluating internal controls, which is critical to the fraud risk assessment process. Consequently, the fraud risk assessment is most effective when management and auditors share ownership of the process and accountability for its success.
**Independence/Objectivity of the People Leading and Conducting the Work**

A good fraud risk assessment can be effectively conducted either by people inside the organization or with external resources. Either way, it is critical that the people leading and conducting the fraud risk assessment remain independent and objective throughout the assessment process. Additionally, they must be perceived as independent and objective by others.

Cultural neutrality is an important aspect of independence and objectivity when leading or conducting a fraud risk assessment. Some organizations have very strong corporate cultures that can play a big role in influencing the way the people inside the organization think about fraud risk. If people within the organization are leading and conducting the fraud risk assessment, they must be able to step outside the corporate culture to assess and evaluate the presence and significance of fraud risks in the business.

**A Good Working Knowledge of the Business**

The individuals leading and conducting the fraud risk assessment need to have a good working knowledge of the business. Every organization is unique; even companies that appear similar have characteristics that differentiate them—and their fraud risks—from their competitors. Some of those differences can be obvious, whereas others are more subtle.

To ensure a good working knowledge of the business, the fraud risk assessor must know, beyond a superficial level, what the business does and how it operates. He must also have an understanding of what makes the
organization both similar to and different from other companies in related lines of business.

Access to People at All Levels of the Organization

It is often said that perception is reality. In other words, how an individual perceives a situation is his reality of that situation. In an organization, it is important that the perceptions of people at all levels are included in the fraud risk assessment process.

Leaders of a business or function often have very different perspectives from their subordinates on how something is perceived or executed; however, this does not mean that one perspective is right and the other is wrong. What it does mean is that expectations and perceptions within the organization are not aligned, which could increase fraud risk.

Risk assessments created and/or performed by management and auditors without the input of the staff performing the operational tasks will be ineffective. If, for example, management puts extensive focus into assessing the risks of large, fine-producing violations, it could easily miss less obvious—though still costly and significant—fraud risks, such as theft of company equipment. Therefore, it is crucial to include members of all levels of the organization in the risk assessment process to ensure that all relevant risks are addressed and reviewed from many different perspectives.

The Ability to Think the Unthinkable

Most honest people are not naturally inclined to think like a fraudster. In fact, many large-scale frauds that have occurred would have been deemed unthinkable by people closest to the events. A good fraud risk assessment requires the people leading and conducting
the assessment to be expansive in their consideration and evaluation of fraud risk; they must constantly ask “what could go wrong?” even in situations where all appears right. Thoughts of “it couldn’t happen here” should not be allowed to moderate the evaluation of fraud risk.

**A Plan to Keep It Alive and Relevant**

The fraud risk assessment should not be treated as a onetime exercise that is executed, reported on, and then put on a shelf to collect dust. The organization should strive to keep the process alive and relevant through ongoing dialogue, active management of action plans, and development of procedures to ensure the assessment is maintained on a current basis.

As part of this ongoing process, any discovered fraud cases should be included in the assessment, with contributing factors being identified and evaluated, and any remedial actions assessed for effectiveness in managing the risk of recurrence.

**Fraud Preventive Controls**

*The Perception of Detection*

Increasing the perception of detection may well be the most effective fraud prevention method. Controls, for example, do little good in forestalling theft and fraud if potential perpetrators do not know about their presence in an organization. Conversely, certain controls that are typically used to detect fraud can also have a deterrent effect by instilling a perception of detection in potential perpetrators’ minds.

**MANAGEMENT OVERSIGHT**

It is common for employees who steal to use the proceeds for lifestyle improvements. Some
examples include: more expensive cars, extravagant vacations, expensive clothing, new or remodeled homes, expensive recreational property, and outside investments. Additionally, fraudsters often display specific behavior red flags during their scheme. Managers should be educated to be observant to these signs.

**REPORTING MECHANISMS AND WHISTLEBLOWER PROGRAMS**

An anonymous reporting channel, such as a third-party fraud hotline or online reporting mechanism, is an integral part of an anti-fraud control system. The combination of an effective reporting method and a staff that’s well-educated in how and why to help detect fraud creates an audit staff of thousands and can potentially be the most effective fraud prevention measure possible.

In educating employees about the reporting program, it should be specifically emphasized that:

- Fraud, waste, and abuse occur in nearly all companies.
- Such conduct costs the company jobs and profits.
- The company actively encourages any employee with information to be able to come forward.
- The employee can come forward and provide information anonymously and without fear of recrimination for good faith reporting.
- There is an exact method for reporting an incident, such as by calling a hotline or a telephone number.
- The report need not be made to one’s immediate superiors.
--- Reports of suspicious activity will be promptly and thoroughly evaluated

**MANDATORY VACATION AND JOB ROTATION POLICIES**
Certain fraudulent acts (e.g., lapping schemes) require that the fraudsters maintain a continual presence in their job position order to conceal their scheme. Requiring that employees take annual vacations, during which time others perform their duties, increases the risk that potential fraudsters will be caught and can have a strong deterrent effect. Similarly, periodically rotating job functions of key employees is an additional anti-fraud measure employers can take—and it comes with the added benefit of having cross-trained employees who can fill in when needed.

**PROACTIVE AUDIT POLICIES**
Proactive audit policies are generated from the top of the operation involved. A proactive policy means that the auditors will aggressively seek out possible fraudulent conduct instead of waiting for instances to come to their attention. Examples of proactive audit policies include increased and targeted use of analytical review, and the inclusion of fraud assessment questioning as part of the audit.

**SURPRISE AUDITS WHERE POSSIBLE**
In addition to regularly scheduled fraud audits, surprise fraud audits of business functions in which fraud is most likely to occur can be effective both in increasing employees’ perception of detection and in uncovering actual frauds that have been perpetrated. The surprise element must be present for this control to be effective; predictability allows

---
perpetrators the time to conceal their acts by altering, destroying, or misplacing records and other evidence.

**Organizational Structure**
A well-designed organizational structure—with key areas of authority and clear and proper lines of reporting—can be an effective preventive measure. A confused structure, in contrast, makes it easier for a fraudster to perpetrate and conceal his misdeeds.

Establishing and communicating the proper flow of information to everyone in the organization is an essential component of a well-designed organizational structure. Flowcharts displaying organizational and departmental hierarchies can be a helpful tool for this purpose. To ensure that information is being properly received and that instructions are being carried out, checks must be established.

**Independent Board of Directors/Audit Committee**
When management knows that its board of directors, including the audit committee, is on the lookout for fraudulent acts—such as management override of controls or inappropriate influence over the financial reporting process—it is less likely to engage in such acts for fear of being caught.

Critical here is that the board be independent of management. A board consisting entirely of management’s cronies is about as useful as a screen door on a submarine.

**Tone at the Top**
Fraud prevention must begin at the top of the organization. *Tone at the top* refers to the ethical
atmosphere that is created in the workplace by the organization’s leadership. Whatever tone management sets will have a trickle-down effect on employees of the company. If the tone set by managers upholds ethics and integrity, employees will be more inclined to uphold those same values. However, if upper management appears unconcerned with ethics and focuses solely on the bottom line, employees will be more prone to commit fraud because they feel that ethical conduct is not a focus or priority within the organization. Employees pay close attention to the behavior and actions of their bosses, and they follow their lead. In short, employees will do what they witness their bosses doing.

**Zero Tolerance**

It must be made clear to employees that the company maintains a policy of zero tolerance for fraud; otherwise, once an employee learns that small frauds are possible, larger frauds might be right around the corner. In addition, by not consistently punishing perpetrators, a company renders its fraud prevention program less effective, if not useless. Having a public record of the incident can also be important, so filing police reports for known incidents of fraud can be an effective step in making the organization’s zero tolerance stance clear.

**Internal Audit Function**

The mere presence of an internal audit function can serve as an effective preventive control. When employees know that internal auditors are actively and aggressively seeking out fraudulent conduct, they are less likely to engage in it. Also, if the internal auditors use continuous auditing software and employees are
DEVELOPING A DYNAMIC AND IMPACTFUL FRAUD PREVENTION PROGRAM

aware of that fact, potential fraudsters might be further deterred.

The internal audit department should have adequate resources and authority to operate effectively and without undue influence from senior management. If the company has a board of directors, the internal audit department should report directly to the board or to the board’s audit committee.

**Employee Education**
A formal fraud education training program is a vital component in increasing employees’ fraud awareness and in preventing and detecting fraud.

Preventing fraud requires ensuring that employees, managers, and those charged with governance understand the red flags of fraud and what actions constitute fraud. In addition, it is important to make clear to these parties the costs of fraud to the organization, including lost profits, adverse publicity, job loss, and decreased morale and productivity.

Fraud training can be accomplished through memoranda, organization-wide e-mails and voice mails, training programs, and other intercompany communication methods. Any education efforts should be positive and non-accusatory. The goal is to make others within the company your eyes and ears.

**Hiring Practices and Promotion Procedures**
By including the following preventive controls in a company’s hiring policy and promotion procedures (where permitted by law), management can minimize its chance of hiring or promoting dishonest and untrustworthy people:
### DEVELOPING A DYNAMIC AND IMPACTFUL FRAUD PREVENTION PROGRAM

- Past employment verification
- Criminal and civil background checks
- Credit check
- Drug screening
- Education and certification verification
- References check
- Periodic training on the organization’s values and code of conduct
- Ongoing evaluation of compliance with the organization’s values and code of conduct

### Minimizing Employee Pressures

Pressures can be especially difficult to detect on the part of the employees. Steps companies can take steps to assist an employee who may be having difficult times include:

- Reasonable performance goals
- Open-door policies
- Employee support programs
- Proper management training
- Career development opportunities
- Special events for employees
- Recognition of employees for a job well done

### Code of Conduct and Ethics Policy

The code of conduct and ethics policy can function as excellent preventive controls if implemented properly with strong communication and management support. Organizations should also consider the costs, benefits, and appropriateness of extending the code of conduct or ethics policy to vendors and agents.

### Fraud Prevention Policy

An unambiguous written fraud policy can be an effective first step toward fraud deterrence. This policy should include at a minimum provisions regarding:
## Developing a Dynamic and Impactful Fraud Prevention Program

- Management’s overall responsibility for fraud
- Who in the organization handles various fraud matters under differing circumstances
- What actions constitute fraud
- The confidential nature of any fraud investigations
- Reporting procedures for suspected fraud
- Sanctions for fraudulent activity

### Monitoring Your Fraud Prevention Program

As with other aspects of the compliance program, the organization’s fraud prevention practices must be constantly monitored, frequently evaluated, and adjusted as needed to reflect the current realities and risks faced by the organization. The performance of the overall program, as well as individual components, can be benchmarked:

- Against management’s expected outcomes
- Against prior trends in fraud prevention and occurrence
- Against industry data and experiences (if available)
- Across business units or functions

### Conclusion

Fraud is a risk that is always present, and it exists in every organization, no matter what industry or size. To protect organizational resources and to set the proper ethical tone, ethics and compliance professionals must adequately and proactively integrate fraud prevention as part of their organization’s compliance, ethics, and risk management process.