

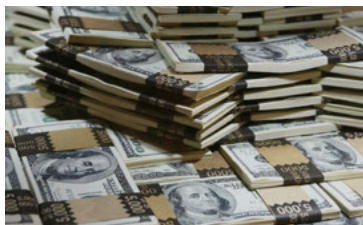


WHITE PAPER

Factors to Consider When Developing a Fraud Detection and Deterrence Program



Succeed. Transform. Compute. Perform.



Fraud takes many forms but it's almost always preventable when an organization has the right policies, procedures and controls securely in place. This paper reviews the origins of fraud and considers best practice prevention.

Understanding fraud and factors to consider when developing a Fraud Detection and Deterrence Program

EXECUTIVE SUMMARY

In today's high-tech world of banking, complex processes – some of which are legacy processes and no longer operating at peak efficiency – are the norm. Design for Six Sigma (DFSS) is one way to bridge the gap between profitability and these cumbersome processes, increasing regulatory requirements and higher overhead costs.

FRAUD DETECTION AND DETERRENCE

Almost every organization must confront the issue of fraud in some shape or form. The precise legal definition of fraud varies by jurisdiction and by the specific fraud offense. In the U.S. legal framework, fraud is a specific offense with certain features. Many criminologists, fraud experts and law enforcement professionals define fraud as: "A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment." As such, fraud includes any intentional or deliberate act to deprive another of property or money by guile, deception, or other unfair means.

According to the Association of Certified Fraud Examiners (ACFE), fraud against an organization can be committed either internally by employees, managers, officers, or owners of the company, or externally by customers, vendors, and other parties. Other schemes defraud individuals, rather than organizations.

There are different types of fraud and many companies continue to see an increase in fraud losses arising from one or more fraudulent activities such as bankruptcy fraud, credit card fraud, mortgage fraud, securities fraud and internet fraud. The Association of Certified Fraud Examiners classifies fraud types as:

- **Internal fraud**, also called *occupational fraud*, can be defined as: "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets." Simply stated, this type of fraud occurs when an employee, manager, or executive commits fraud against his or her employer.

- **External fraud** against a company includes a broad range of schemes. Dishonest vendors might engage in bid-rigging schemes, bill the company for goods or services not provided, or demand bribes from employees. Likewise, dishonest customers might submit bad checks or falsified account information for payment, or might attempt to return stolen or knock-off products for a refund. In addition, organizations face threat of security breaches and thefts of intellectual property perpetrated by unknown third parties. Other examples of fraud committed by external third parties include hacking, theft of proprietary information, tax fraud, bankruptcy fraud, insurance fraud, healthcare fraud, and loan fraud.
- **Fraud against individuals.** Numerous fraudsters have also devised schemes to defraud individuals. Identity theft, Ponzi schemes, phishing schemes, and advanced-fee frauds are just a few of the ways criminals have found to steal money from unsuspecting victims.



The fraud triangle is the most widely accepted model for explaining why people commit fraud. This model was developed by Dr. Donald Cressey, a criminologist whose research focused on embezzlers—people he called “trust violators.” The fraud triangle model explains factors that cause someone to commit occupational fraud. Together, its components of perceived unshareable financial need, perceived opportunity and rationalization lead to fraudulent behavior.

HOW ORGANIZATIONS CAN DETECT AND PREVENT FRAUD.

As fraud losses increase, companies can proactively develop and implement robust and effective fraud detection and deterrence programs. A key element of an effective fraud detection and deterrence program is a Fraud Risk Assessment.

WHAT IS A FRAUD RISK ASSESSMENT?

A Fraud Risk Assessment examines the internal controls, policies and procedures of an organization to identify weaknesses which could be exploited by management team members, employees, vendors or outside perpetrators. The assessment team determines if management and employees are aware of and practice these policies in their day to day work, and confirm through testing that they are being practiced. Fraud risk assessment methodology is broken down into modules; each module examines a specific business function and the assessment team looks for vulnerabilities in areas where fraud is most likely to occur. The assessment team will identify and document weaknesses and develop recommendations for remediation.

Fraud experts suggest that the most cost-effective way to limit fraud losses is to utilize a Fraud Prevention Checklist. This checklist helps organizations test the effectiveness of their fraud prevention measures. This sample checklist focuses primarily on employee fraud awareness, internal controls, reporting and training.

FRAUD PREVENTION CHECKLIST

☐ **Is ongoing anti-fraud training provided to all employees of the organization?**

Do employees understand what constitutes fraud?

☐ **Have the costs of fraud to the company and everyone in it – including lost profits, adverse publicity, job loss, and decreased morale and productivity – been made clear to employees?**

Do employees know where to seek advice when faced with uncertain ethical decisions, and do they believe that they can speak freely?

Has a policy of zero-tolerance for fraud been communicated to employees through words and actions?

☐ **Is an effective fraud reporting mechanism in place?**

Have employees been taught how to communicate concerns about known or potential wrongdoing?

Is there an anonymous reporting channel, such as a third-party hotline, available to employees?

Do employees trust that they can report suspicious activity anonymously and/or confidentially and without fear of reprisal?

Has it been made clear to employees that reports of suspicious activity will be promptly and thoroughly evaluated?

Do reporting policies and mechanisms extend to vendors, customers and other outside parties?

☐ **To increase employees' perception of detection, are the following proactive measures taken and publicized to employees?**

Is possible fraudulent conduct aggressively sought out, rather than dealt with passively?

Does the organization send the message that it actively seeks out fraudulent conduct through fraud assessment questioning by auditors?

Are surprise fraud audits performed in addition to regularly scheduled audits?

Is continuous auditing software used to detect fraud and, if so, has the use of such software been made known throughout the organization?

☐ **Is the management climate/tone at the top one of honesty and integrity?**

Are employees surveyed to determine the extent to which they believe management acts with honesty and integrity?

Are performance goals realistic?

Have fraud prevention goals been incorporated into the performance measures against which managers are evaluated and that are used to determine performance-related compensation?

Has the organization established, implemented and tested a process for oversight of fraud risks by the board of directors or others charged with governance (e.g., the audit committee)?

☐ **Are strong anti-fraud controls in place and operating effectively, including the following?**

Proper separation of duties

Use of authorizations

Physical safeguards

Job rotations

Mandatory vacations

☐ **Does the internal audit department, if one exists, have adequate resources and authority to operate effectively and without undue influence from senior management?**

☐ **Does the hiring policy include the following (as permitted by law)?**

Past employment verification

Criminal and civil background checks

Credit checks

Drug screening

Education verification

Reference checks

☐ **Are employee support programs in place to assist employees struggling with addiction, mental/emotional health, family or financial problems?**

☐ **Is an open-door policy in place that allows employees to speak freely about pressures, providing management the opportunity to alleviate such pressures before they become acute?**

☐ **Are anonymous surveys conducted to assess employee morale?**

☐ **Are fraud risk assessments performed to proactively identify and mitigate the company's vulnerabilities to internal and external fraud?**

PREVENTION STARTS WITH ASSESSMENT

Identifying risk is the first step to loss prevention. That's as true for fraud loss as for any other type of loss. A formal fraud risk assessment program is the first step towards protection for competitive advantage, proprietary assets, shareholder relations, regulatory compliance and disruption prevention. With adequate policies and procedures and an effective internal control framework in place, organizations are able to focus on operating a business instead of fighting breaches, theft and all the other forms fraud can take.