

Business Consulting

- Regulatory Support
 - Policies and Procedures
 - Regulatory Compliance
 - Sarbanes-Oxley
 - GLBA
 - HIPAA
 - BSA
 - PCI (Payment Card Industry) Security Audit
 - Information System Audit Outsourcing
- Enterprise Support
 - Business Continuity Planning
 - Attestation and Assurance
 - SAS-70
 - E - Discovery
 - Forensic Examinations
 - Security Remediation

Technology Consulting

- Application Security
 - Application Security Assessment
 - Application Penetration Test
 - Web Application Security Assessment
 - Web Application Penetration Test
- Network Security
 - Risk Assessment
 - Vulnerability Assessment
 - Penetration Testing
 - Internal
 - External
 - Social Engineering
 - War Dialing
 - War Driving
 - Blue Snarfing
 - Wireless Security Assessment
 - Information System Security Audit
 - Information System Control Audit
 - Network Architecture Design and Assessment
 - Physical Security Assessment
 - Log Analysis

Control Essentials

Volume II, Issue IX

September 2007

Anti-Fraud Programs

Introduction

Fraud arises in many different contexts. In general, fraud includes any conduct or course of conduct that is deceitful, and ordinarily results in a loss to another or in a gain to the person or entity engaged in the fraudulent conduct.

Studies indicate that there has been a substantial increase in the occurrence of fraud in the United States. U.S. companies lose an estimated six percent of their revenue to frauds (an average of 600 billion dollars only in the U.S.). In addition to financial loss, incidents of fraud also affect stockholder trust, employee morale and most importantly, the reputation of the company. These studies also reveal that some of the most common fraud schemes are fairly simple and that all organizations, irrespective of their size, may become a victim of fraud.

In recent years, there have been highly publicized incidents of fraud involving major organizations. This has led to increased pressure on all organizations to step up their efforts to fight fraud. Laws, regulations and auditing standards now require organizations to develop effective Anti-Fraud Programs to counter fraud, some of them being:

- The Sarbanes Oxley Act
- Securities and Exchange Commission (SEC) regulations
- American Institute of Certified Public Accountants (AICPA) Statement of Auditing Standards (SAS) 99
- Public Company Accounting Oversight Board (PCAOB) Auditing Standard 5

Because of the increased incidence of fraud as well as the new legal requirements and standards, organizations recognize the need to implement Anti-Fraud Programs in order to prevent, deter and detect frauds.

Essential Components of an Anti-Fraud Program

An effective Anti-Fraud Program requires the coordinated effort of the board of directors, management, the internal audit department, and independent auditors. It needs to address methods for the prevention, deterrence and detection of fraud.

Fraud prevention and deterrence measures are the most effective and the least costly. On the other hand, detecting frauds can be complicated. Also, fraud investigations can be time consuming and costly. Therefore, organizations can benefit greatly from Anti-Fraud Programs that are focused on the prevention and deterrence of fraudulent incidents.

Anti-Fraud programs require the following five components:

- A culture of honesty and high ethics
- A Whistleblower Program
- A Corporate Fraud Policy
- A Fraud Risk Assessment
- An oversight process



Culture of Honesty and High Ethics

The ethical values prevalent in an organization have their foundation in the organization's Code of Conduct. The Code of Conduct is a statement that describes the values of an organization, including ethics, confidentiality, conflicts of interest, intellectual property, sexual harassment, and fraud. Organizations should make the Code of Conduct accessible to all employees through the organization's Intranet and Policy Manual.

A company's culture can also be significantly influenced by the employees' perception of their workplace. Dissatisfaction with the company may serve as a motivating factor for employees to commit fraud against it. It is therefore important to take employees into consideration in the development of the Code of Conduct.

Furthermore, organizations should make it mandatory for newly hired employees to attend training sessions to increase "fraud awareness". Such sessions should cover topics such as fraud identification and fraud reporting. Management should adopt a policy of "no tolerance" towards fraud and should periodically remind employees through the use of newsletters. Newsletters are also a powerful means to announce deterred frauds and reward employees for ethical conduct.

Whistleblower Program

Employees should be given ample opportunity to voice their opinions and concerns. The purpose of a Whistleblower Program would be to:

- Provide a means of communicating concerns related to potential events of fraud, violations of the code of conduct or unethical behavior, without the fear of a backlash.
- Provide advice prior to making decisions with substantial legal and ethical implications.

Upon receipt of information about an identified unethical activity, a whistleblower program should have specific procedures for dealing with the complaints. Having a program that does not address the complaints received is as good as not having one at all.

Corporate Fraud Policy

The code of conduct needs to be reinforced by a well-written Corporate Fraud Policy. Generally, a corporate fraud policy addresses at least the following issues:

- The responsibilities and roles for deterring, detecting and investigating fraud.
- Procedures for handling and reporting fraud to the appropriate individuals.
- Procedures for rewarding employees.
- Procedures for publishing the results of fraud investigations.
- Involvement of legal and law enforcement agencies.
- Prosecution of the individuals committing fraud.

Additionally, organizations should also have policies and procedures in place for employee hiring and promotion to minimize the chance of hiring or promoting dishonest individuals. Activities may include:

- Background investigations.
- Education and employment history checks.
- Periodic training about the corporate system values and the code of conduct.
- Regular job performance reviews.

Furthermore, the corporate fraud policy should require all employees to sign the code of conduct and a statement affirming that the individual understands and has complied with the corporate code of conduct. This should be done at least annually.

Fraud Risk Assessment

Organizations should be proactive in reducing fraud opportunities by identifying and measuring fraud risks. This can be done through a Fraud Risk Assessment that is proportional to the complexity and size of an organization and should cover all the vulnerabilities of the organization to fraudulent activity. Fraud Risk Assessments involve examination of existing controls just like traditional risk assessments; however, they focus on control measures aimed at preventing and detecting fraud. Extra care should be taken to investigate whether these controls can be overridden by management.

More importantly, Fraud Risk assessments focus on the possible fraud scenarios. Assessments are geared towards identifying activity that can result in financial loss, or expose the organization to reputational risk and litigation.



Upon completion of the Fraud Risk Assessment, the organization can identify the processes, controls, and procedures necessary to mitigate the identified risks. Because of the importance of information technology in supporting operations and transactions, the risk assessment should also address issues such as IT and security controls.

Oversight Process

An appropriate oversight process is fundamental to prevent and deter frauds. The oversight process requires the cooperation of management, board of directors, internal auditors, and independent auditors. While management is responsible for overseeing the activities carried out by employees, the board of directors ensures that management has taken action to protect investors and employees. The involvement of the board of directors reinforces the organizational commitment to fostering a culture of “no tolerance” towards fraud by setting the “tone at the top”.

In order to provide for a fundamental security layer to detect and deter fraud, an internal audit team may be used. Also, independent auditors can provide an assessment of the entity’s process for identifying, assessing, and responding to the risks of fraud.

Conclusion

Organizations should be proactive in implementing Anti-Fraud Programs. An Anti-Fraud Program is a coordinated effort that requires time and the active participation of all the key players within an organization. Anti-Fraud Programs can be implemented as a response to a fraud incident, however, it is highly recommended to include a fraud risk assessment as part of the regular activities of risk management. The greatest benefit of an effective Anti-Fraud Program will be tangible in the long run: an organization with high ethics, less risk of fraud, and employees who are equipped to identify and respond to fraud if necessary.

Their consultants are more seasoned than typical *Big 4* firms.



Known technical quality at less than *Big 4* firm rates.

We selected ERM because of their professional references, experience and reasonable professional fees.



ERM accomplished and exceeded objectives planned.

They have the ability to understand the needs of our organization and work well with our employees.



Enterprise Risk Management At A Glance

ERM professionals bring a unique mix of strong academic backgrounds complemented by professional experience ranging from "Big Four" consulting firms to major corporations and prestigious professional certifications. A snapshot of ERM's profile can be seen below:

Education

Qualifications

M. S. in Computer Information Systems
M. S. in Information Networking
M. S. in Management Information Systems
Master of Accounting Information Systems
Master of Business Administration

Universities

Carnegie Mellon University, Pittsburgh, Pennsylvania
Syracuse University, Syracuse, New York
Xavier University, Cincinnati, Ohio
University of Miami, Miami, Florida
Florida International University, Miami, Florida

Certifications

Certified Public Accountant (CPA)
Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)
Certified Information Systems Manager (CISM)
Certified Information Technology Professional (CITP)
GIAC Security Essentials Certification
GIAC Systems and Network Auditor
Microsoft Certified Professional

Prior Work Experience

PriceWaterhouse Coopers
CERT® Coordination Center
SONY Electronics Latin America, Inc.
RJR Nabisco
Diageo plc
Arthur Young
Carnegie Mellon CyLab
Evertec Inc.
American Bankers Insurance Group
Chesebrough Pond's
Starboard Cruise Services, Inc.
Demotte Consulting, Ltd.

Some of our Clients...

ABN AMRO Private Banking
Bacardi-Martini, Inc.
CitiBank
Carnival Cruise Lines
Commerce Bank
Florida Power & Light Company
Knight Ridder
North Broward Hospital District
Ocean Bank
Rinker Materials
Sylvania Lighting International
The International Bank of Miami

KEEPING WATCH OVER YOUR BEST BUSINESS INTERESTS

enterprise risk management

The Control Professionals

299 Alhambra Circle, Suite 220,
Coral Gables, FL 33134.
P: (305) 447 6750 F: (305) 447 6752
Email: info@emrisk.com Web: www.emrisk.com