The Internal Controls Pyramid demonstrates how each process is reliant on the others, starting with the foundation of the Control Environment. Should any of the processes fail, the effectiveness of the remaining processes is weakened and the risk of fraud or significant financial damage to the organization as a result of fraud is increased.

Roles in Fraud Detection

Internal auditors are responsible for providing assistance to prevent fraud by examining and evaluating the adequacy and effectiveness of their internal controls system, commensurate with the extent of a potential exposure within the organization. When meeting their responsibilities, internal auditors should consider the following:

- Control Environment – Assess aspects of the control environment through proactive audits and investigations.
- Fraud Risk Assessment – Evaluate management's fraud risk assessment, in particular its process for identifying, assessing, and testing potential fraud and misconduct schemes, including those involving contractors and suppliers.
- Control Activities – Assess the design and operating effectiveness of fraud-related controls.
- Information and Communication – Assess the operating effectiveness of information communication systems and practices.
- Monitoring – Assess monitoring activities and related computer software.

Management is responsible for establishing and maintaining an effective control system at a reasonable cost. This includes designing some controls to indicate when other controls are not working effectively. Following up on these indicators may result in the determination that fraud may have occurred. Tests conducted by auditors improve the likelihood that any existing fraud indicators or "red flags" will be detected and considered for further investigation; however, audits cannot guarantee an absence of fraud.

Department of Elder Affairs

Taroub J. Faraj, Inspector General
850-414-2013

Kimberly Jones, Director of Internal Audit
850-414-2117

Office of Inspector General
4040 Esplanade Way
Tallahassee, FL 32399
Phone: 850-414-2000
Fax: 850-414-2301

http://elderaffairs.state.fl.us/doea/ig.php

Department of Elder Affairs
State of Florida

Office of Inspector General

Fraud

The Responsibilities of Management and Auditors

Source of Information
The American Institute of Certified Public Accountants Statement on Auditing Standards

The Institute of Internal Auditors
The Professional Practices Framework

Inspector General
Taroub J. Faraj

What is fraud?

Fraud encompasses a range of irregularities and illegal acts characterized by intentional deception or misrepresentation that an individual knows to be false or does not believe to be true. Fraud is perpetrated by a person knowing that it could result in some unauthorized benefit to him or her, to the organization, or to another person, and it can be perpetrated by persons outside and inside the organization. Fraud perpetrated to the direct or indirect benefit of an employee or outside party will generally have a detrimental effect on the organization. Some examples include the following:

- Embezzlement of money or property;
- A profitable transaction diverted to an employee or outsider that would typically generate profits for the organization;
- Claims submitted for goods or services not provided;
- Unauthorized or illegal use of proprietary information; or
- Theft.

Fraud designed to benefit the organization generally produces benefit by exploiting an unfair or dishonest advantage. This type of fraud may also indirectly benefit an individual through bonus payments or promotions and may include the following:

- Intentionally presenting an enhanced picture of the financial status of the organization;
- Improper payments, such as illegal political contributions;
- Intentional misrepresentation of valuation of transitions, assets, liabilities, and income;
- Intentional errors in tax compliance activities to reduce taxes owed; or
- Sale of fictitious or misrepresented assets.

Why does fraud occur?

There are generally three factors that influence the commission of fraud.

- **Opportunity** – A window of opportunity for fraud may exist due to poor control design, a lack of controls, or controls that can be easily circumvented by management. Controls may also lose their effectiveness and must be constantly reevaluated to assess their value and limit opportunity.
- **Incentive** – Also known as motive, a person's incentive for committing fraud may be linked to power, greed, or pressure. Power is a great motivator for those who desire esteem in the eyes of others. For example, many computer frauds are committed to show that the hacker has the power to do it rather than to cause intentional harm. Other motivators include greed, which is simply the gratification of the person's desire to accumulate wealth, and pressure, such as financial stress and need for money.
- **Rationalization** – An attitude that allows individuals to knowingly and intentionally commit or justify a dishonest act. Rationalizations can include a sense of entitlement by the person, the intent to return stolen funds once a financial burden is relieved, or the depersonalization of the act through the belief that the company can handle the loss.

THE FRAUD TRIANGLE

Breaking the Triangle

To break the fraud triangle, one of the three elements of fraud must be removed. Although management and auditors may not be able to know the exact **incentive** or **rationalization** leading to fraud, they are expected to understand enough about internal controls to identify and eliminate **opportunities** for fraud.

Fraud Prevention and Deterrence

There are five components that are essential to fraud prevention and deterrence. As each process is refined and improved upon by management, with assistance from an internal audit, the likelihood of eliminating opportunity for fraud increases.

- **Control Environment** – Organizations must develop and maintain an appropriate environment of conduct, ethics, attitudes, and philosophies intent on deterring, detecting, and eliminating fraudulent activities. Management should set the tone for intolerance of fraud by developing a code of conduct, a detailed ethics policy, and a method for reporting and investigating violations.
- **Fraud Risk Assessment –** Organizations must develop and maintain a fraud risk assessment that identifies and assesses threats to the organization, such as the potential for fraudulent financial reporting, asset misappropriations, improper receipts or expenditures, or financial misconduct by staff including senior management.
- **Control Activities –** A control is any process or action taken by management to ensure the organization's goals and objectives are achieved. Simply put, strong controls that are properly developed, maintained, and implemented will keep an organization on track and likely deter fraudulent activities. Controls include appropriate separation of duties, strong policies and procedures, adequate forms and authorizations for certain tasks, physical asset protection, and independent review of performance.
- **Information and Communication –** Organizations must develop a method of communication that allows for the greatest exchange of ideas and information. Proper communication enables maximum operational efficiency as information will flow up, down, and across the organization.
- **Monitoring –** Monitoring involves the proactive review and assessment of internal controls to ensure they are functioning appropriately and optimally. Organizations must have a monitoring method in place to ensure the effectiveness of adequate controls is not reduced or circumvented.