

The Five Principles of Fraud Risk Management

Information courtesy of *Managing the Business Risk of Fraud: A Practical Guide*, a joint project of the Institute of Internal Auditors, the American Institute of Certified Public Accountants and the Association of Certified Fraud Examiners. The guide suggests that organizations follow five principles to manage their risk of fraud. While written to address the needs of private-sector businesses, these roles can easily be applied to government entities.

1. Fraud Risk Governance

As part of an organization's governance structure, a fraud risk management program should be in place, including a written policy (or policies) to convey the expectations of the board of directors and senior management regarding managing fraud risk.

- Management must set the tone for the rest of the organization and make fraud risk management a priority.
- Make it official. Organizations should have a formal fraud risk management program, including written policies and procedures.
- Management should adjust their fraud risk management program to fit the specific characteristics and needs of their organization.

2. Fraud Risk Assessment

Fraud risk exposure should be assessed periodically by the organization to identify specific potential schemes and events that the organization needs to mitigate.

- Fraud risk management is not a one-time development. An organization's plan should be re-evaluated and updated regularly.
- A fraud risk assessment should include an evaluation of the incentives, pressures and opportunities to commit fraud within the organization.
- Evaluating the risk of fraud should also include an examination of management, including internal controls and segregation of duties.

3. Fraud Prevention

Prevention techniques to avoid potential key fraud risk events should be established, where feasible, to mitigate possible impacts on the organization.

- Not all fraud is preventable. However, preventive techniques are an organization's first line of defense against fraud.
- Financial controls are not fraud controls. Therefore, an organization should develop a specific set of preventive measures designed to address fraud risk.
- The success of preventive techniques is reliant on awareness and reinforcement.

4. Fraud Detection

Detection techniques should be established to uncover fraud events when preventive measures fail or unmitigated risks are realized.

- Detection techniques are not designed to prevent fraud, but they do work as a check to ensure prevention techniques are working as intended.
- Detection techniques will act as a deterrent against fraud, but only if they are properly designed, visible and effective.
- Detection techniques should be flexible and adaptable to meet changing risks of fraud.

5. Investigation and Corrective Action

A reporting process should be in place to solicit input on potential fraud, and a coordinated approach to investigation and corrective action should be used to help ensure potential fraud is addressed appropriately and timely.

- A documented and timely investigative and corrective action process can improve an organization's chances of recovering loss, minimizing exposure to litigation and lessening damage to reputation.
- Management should establish a specific protocol for receiving, evaluating, tracking and investigating fraud allegations.
- The investigation and corrective action process must be a coordinated effort between management and other areas of the organization, including legal, human resources and others.