Highlights of GAO-15-593SP, a Framework for Managing Fraud Risks

July 2015

A Framework for Managing Fraud Risks in Federal Programs

What GAO Found

To help managers combat fraud and preserve integrity in government agencies and programs, GAO identified leading practices for managing fraud risks and organized them into a conceptual framework called the Fraud Risk Management Framework (the Framework). The Framework encompasses control activities to prevent, detect, and respond to fraud, with an emphasis on prevention, as well as structures and environmental factors that influence or help managers achieve their objective to mitigate fraud risks. In addition, the Framework highlights the importance of monitoring and incorporating feedback, which are ongoing practices that apply to all four of the components described below.

Why GAO Did This Study

Fraud poses a significant risk to the integrity of federal programs and erodes public trust in government. Managers of federal programs maintain the primary responsibility for enhancing program integrity. Legislation, guidance by the Office of Management and Budget (OMB), and new internal control standards have increasingly focused on the need for program managers to take a strategic approach to managing improper payments and risks, including fraud. Moreover, GAO's prior reviews highlight opportunities for federal managers to take a more strategic, risk-based approach to managing fraud risks and developing effective antifraud controls. Proactive fraud risk management is meant to facilitate a program's mission and strategic goals by ensuring that taxpayer dollars and government services serve their intended purposes.

The objective of this study is to identify leading practices and to conceptualize these practices into a risk-based framework to aid program managers in managing fraud risks. To address this objective, GAO conducted three focus groups consisting of antifraud professionals. In addition, GAO interviewed federal Offices of Inspector General (OIG), national audit institutions from other countries, the World Bank, the Organisation for Economic Co-operation and Development, as well as antifraud experts representing private companies, state and local audit associations, and nonprofit entities. GAO also conducted an extensive literature review and obtained independent validation of leading practices from program officials.

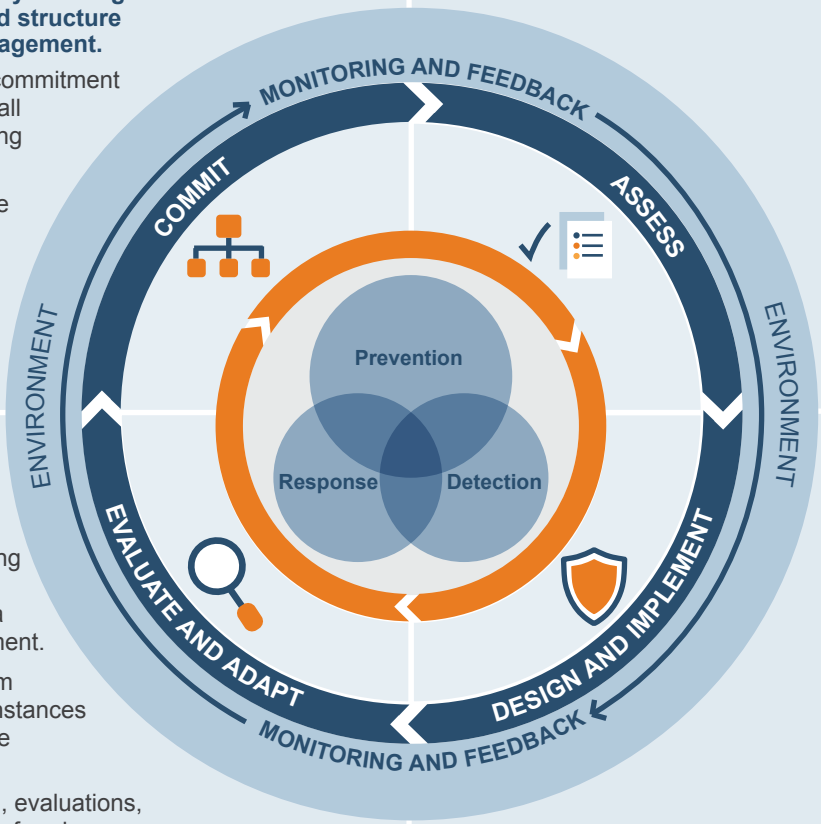
The Fraud Risk Management Framework and Selected Leading Practices

Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.

- Demonstrate a senior-level commitment to combat fraud and involve all levels of the program in setting an antifraud tone.
- Designate an entity within the program office to lead fraud risk management activities.
- Ensure the entity has defined responsibilities and the necessary authority to serve its role.

Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.

- Tailor the fraud risk assessment to the program, and involve relevant stakeholders.
- Assess the likelihood and impact of fraud risks and determine risk tolerance.
- Examine the suitability of existing controls, prioritize residual risks, and document a fraud risk profile.



Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.

- Conduct risk-based monitoring and evaluation of fraud risk management activities with a focus on outcome measurement.
- Collect and analyze data from reporting mechanisms and instances of detected fraud for real-time monitoring of fraud trends.
- Use the results of monitoring, evaluations, and investigations to improve fraud prevention, detection, and response.

Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.

- Develop, document, and communicate an antifraud strategy, focusing on preventive control activities.
- Consider the benefits and costs of controls to prevent and detect potential fraud, and develop a fraud response plan.
- Establish collaborative relationships with stakeholders and create incentives to help ensure effective implementation of the antifraud strategy.

Source: GAO. | GAO-15-593SP

2 Plan Regular Fraud Risk Assessments and Assess Risks to Determine a Fraud Risk Profile

Table 2: Leading Practices for Planning and Conducting Fraud Risk Assessments

2.1 Plan Regular Fraud Risk Assessments That Are Tailored to the Program
Tailor the fraud risk assessment to the program.
Plan to conduct fraud risk assessments at regular intervals and when there are changes to the program or operating environment, as assessing fraud risks is an iterative process.
Identify specific tools, methods, and sources for gathering information about fraud risks, including data on fraud schemes and trends from monitoring and detection activities.
Involve relevant stakeholders in the assessment process, including individuals responsible for the design and implementation of fraud controls.
2.2 Identify and Assess Risks to Determine the Program's Fraud Risk Profile
Identify inherent fraud risks affecting the program.
Assess the likelihood and impact of inherent fraud risks. • Involve qualified specialists, such as statisticians and subject-matter experts, to contribute expertise and guidance when employing techniques like analyzing statistically valid samples to estimate fraud losses and frequency. • Consider the nonfinancial impact of fraud risks, including impact on reputation and compliance with laws, regulations, and standards.
Determine fraud risk tolerance.
Examine the suitability of existing fraud controls and prioritize residual fraud risks.
Document the program's fraud risk profile.

Source: GAO. | GAO-15-593SP

Managers who effectively manage fraud risks develop and document an antifraud strategy that describes the program's approach for addressing the prioritized fraud risks identified during the fraud risk assessment. The antifraud strategy describes existing fraud control activities as well as any new control activities a program may adopt to address residual fraud risks. *Federal Internal Control Standards* notes that documentation of the internal-control system helps establish and communicate to employees the "who, what, when, where, and why" of control implementation.[47] Managers may decide to develop an agency-wide antifraud strategy, or direct individual programs to develop a strategy at the program level. Similar to the fraud risk assessment process, factors such as a program's size, complexity, maturity, and types of fraud risks can inform this decision. Regardless of their application across an agency or for specific programs, effective antifraud strategies reflect the leading practices described in table 4.

Table 4: Key Elements of an Antifraud Strategy

Who is responsible for fraud risk management activities?	Establish roles and responsibilities of those involved in fraud risk management activities, such as the antifraud entity and external parties responsible for fraud controls, and communicate the role of the Office of Inspector General (OIG) to investigate potential fraud.
What is the program doing to manage fraud risks?	Describe the program's activities for preventing, detecting, and responding to fraud, as well as monitoring and evaluation.[a]
When is the program implementing fraud risk management activities?	Create timelines for implementing fraud risk management activities, as appropriate, including monitoring and evaluations.
Where is the program focusing its fraud risk management activities?	Demonstrate links to the highest internal and external residual fraud risks outlined in the fraud risk profile.
Why is fraud risk management important?	Communicate the antifraud strategy to employees and other stakeholders, and link antifraud efforts to other risk management activities, if any.

Source: GAO. | GAO-15-593SP

[a]According to *Federal Internal Control Standards*, control activities are the policies, procedures, techniques, and mechanisms that enforce managers' directives to achieve the program's objectives and address related risks. Broadly speaking, the antifraud strategy itself can be viewed as a preventive control activity, although it can inform other control activities, such as the content of fraud-awareness training or the design of system edit checks. The antifraud strategy describes existing fraud control activities, as well as any new control activities a program may have planned or adopted to address any residual fraud risks.