Using GAO's Fraud Risk Management Framework

Southeastern and Southwest Intergovernmental Audit Forums
September 17, 2015

Linda S. Miller
Assistant Director, Homeland Security and Justice (HSJ)
U.S. Government Accountability Office

Why Is Fraud Risk Management Important?

- Fraud poses a significant risk to the integrity of federal programs and erodes public trust in government.

- Fraud can be financial as well as nonfinancial (e.g., passport fraud), and it is difficult to measure fraud in a reliable way.

- Based on our prior reviews, we saw a need for federal managers to take a more strategic, risk-based approach to managing fraud risks.

- Effective fraud risk management helps to ensure that federal programs' services fulfill their intended purpose, funds are spent effectively, and assets are safeguarded.

How Did GAO Develop the Framework?

- To develop the Framework, we

  - conducted three **focus groups** with antifraud professionals;

  - **interviewed** eight federal Offices of Inspector General, three national audit institutions, the World Bank, the Organisation for Economic Co-Operation and Development, and antifraud experts representing private companies, state and local audit associations, and nonprofit entities;

  - conducted an extensive **literature review**; and

  - independently **validated** leading practices from federal program officials.

The Fraud Risk Management Framework

Source: GAO. | GAO-15-593SP
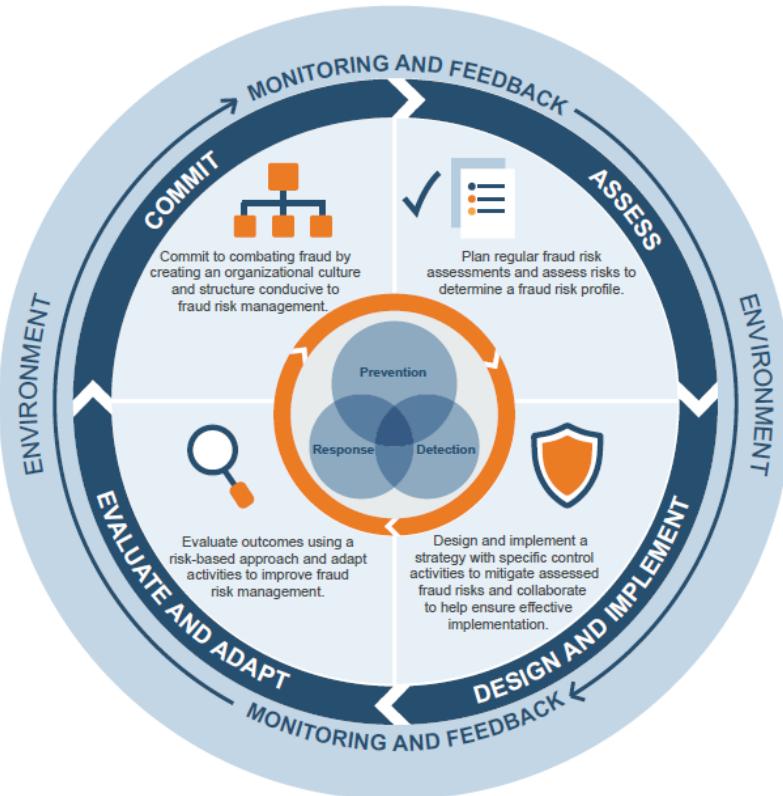
The Framework

- encompasses control activities to **prevent, detect, and respond** to fraud, with an emphasis on prevention;

- recognizes **environmental factors** that influence or help managers achieve their objective to mitigate fraud risks; and

- highlights the importance of **monitoring and incorporating feedback.**

What Are the Components of the Framework?

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

- **Assess**: Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.

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

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

What Are the Components of the Framework? (continued)

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

- **Assess**: Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.

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

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

How Can Managers Assess Fraud Risks?

- **Identify** fraud risks and **assess** their likelihood and impact.

- **Determine fraud risk tolerance**, and **examine existing fraud controls**.

- **Document** the program's **fraud risk profile**, including risk tolerance, prioritization of risks, and other key findings and conclusions.

Figure 4: Key Elements of the Fraud Risk Assessment Process

Universe of Potential Fraud Risks

Inherent Risks

1 Identify inherent fraud risks affecting the program
Managers determine where fraud can occur and the types of fraud the program faces, such as fraud related to financial reporting, misappropriation of assets, or corruption. Managers may consider factors that are specific to fraud risks, including incentives, opportunity, and rationalization to commit fraud.

2 Assess the likelihood and impact of inherent fraud risks
Managers conduct quantitative or qualitative assessments, or both, of the likelihood and impact of inherent risks, including the impact of fraud risks on the program's finances, reputation, and compliance. The specific methodology managers use to assess fraud risks can vary by program because of differences in missions, activities, capacity, and other factors.

3 Determine fraud risk tolerance
According to *Standards for Internal Control in the Federal Government,*[a] risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. In the context of fraud risk management, if the objective is to mitigate fraud risks—in general, to have a very low level of fraud—the risk tolerance reflects managers' willingness to accept a higher level of fraud risks, and it may vary depending on the circumstances of the program.

Prioritized Residual Risks

4 Examine the suitability of existing fraud controls and prioritize residual fraud risks
Managers consider the extent to which existing control activities mitigate the likelihood and impact of inherent risks. The risk that remains after inherent risks have been mitigated by existing control activities is called residual risk. Managers then rank residual fraud risks in order of priority, using the likelihood and impact analysis, as well as risk tolerance, to inform prioritization.

5 Document the program's fraud risk profile
Effectively assessing fraud risks involves documenting the key findings and conclusions from the actions above, including the analysis of the types of fraud risks, their perceived likelihood and impact, risk tolerance, and the prioritization of risks.

Source: GAO. | GAO-15-593SP

[a]GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G (Washington, D.C.: Sept. 10, 2014), 6.08.

What Are the Components of the Framework? (continued)
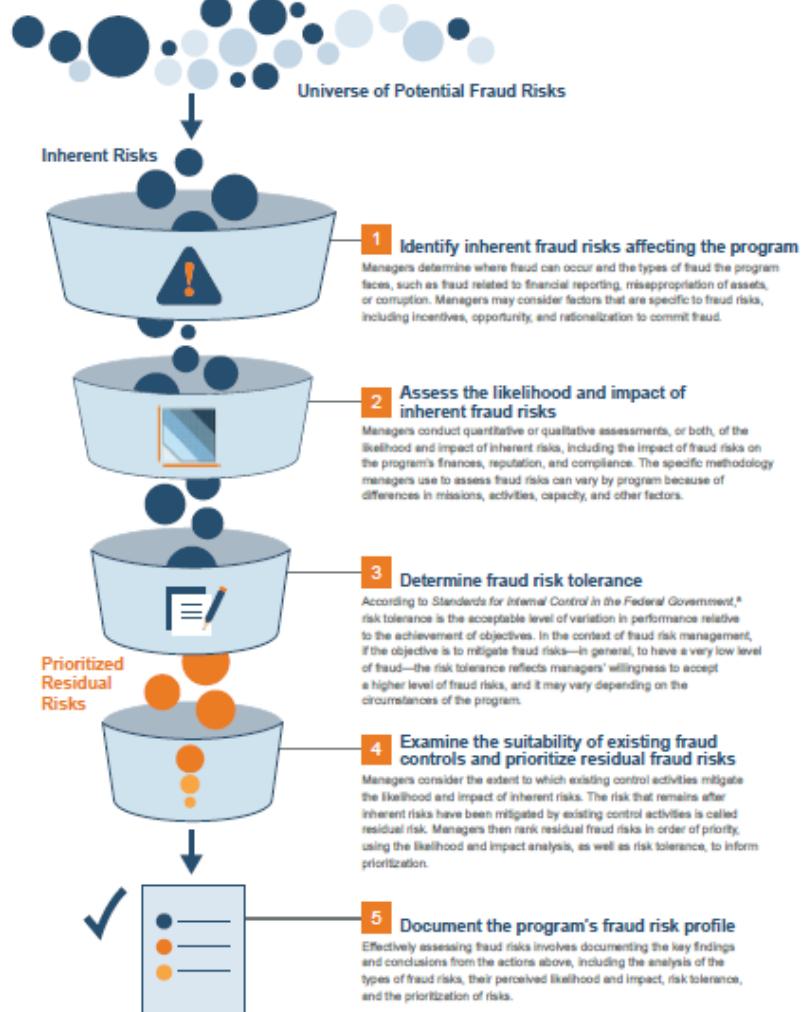
- **Commit**: Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.

- **Assess**: Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.

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

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

What Are the Components of the Framework? (continued)

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

- **Assess**: Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.

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

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

Who Can Use the Framework?

- The Framework's leading practices serve as a guide for **federal program managers** to use when developing or enhancing efforts to combat fraud in a strategic, risk-based manner.

  - Managers can use the Framework to help implement Principle 8 of *Standards for Internal Control in the Federal Government* – "Assess Fraud Risks."

  - Managers can tailor the Framework to their programs' operations and environment, including existing risk management efforts.

How Can Others Use the Framework?

- **Auditors** can use the Framework to help assess managers' fraud risk management efforts.

- **Managers of state, local, and foreign government agencies**, as well as **managers of nonprofit entities**, may find the Framework's concepts and practices useful for their fraud risk management efforts.

How Does the Framework Relate to Existing Federal Efforts to Combat Fraud?

- The Framework complements existing federal efforts, including

    - the revised *Standards for Internal Control in the Federal Government* (effective Oct. 1, 2015);

    - improper-payments legislation; and

    - Office of Management and Budget guidance on improper payments (OMB A-123).

- However, the Framework is fraud-specific and applies to nonfinancial, as well as financial, fraud risks.

Next Steps

- Federal program managers can begin using the Framework immediately to develop or improve fraud risk management efforts.

- However, fraud risk management is an iterative process. Managers may focus on one or two components to start. Over time, as the fraud risk management program evolves, managers will be more likely to effectively address all key elements.

- Internal and external auditors can evaluate the effectiveness of agency fraud risk management efforts and make recommendations to enhance those efforts using the framework as a basis.

Questions?

- For further information:

  - *A Framework for Managing Fraud Risks in Federal Programs* is available online at: http://www.gao.gov/products/GAO-15-593SP.

  - Contact:

    Stephen M. Lord
    (202) 512-6722
    lords@gao.gov

    Linda S. Miller
    (202) 512-6124
    millerls@gao.gov

GAO on the Web

Web site: http://www.gao.gov/

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov
(202) 512-4400, U.S. Government Accountability Office
441 G Street, NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov
(202) 512-4800, U.S. Government Accountability Office
441 G Street, NW, Room 7149, Washington, DC 20548